Developing an artefact for raising social engineering awareness among administrative staff

IL Ngqoyiyana

orcid.org 0000-0002-4241-8160

Dissertation accepted in fulfilment of the requirements for the degree *Master of Science in Computer Science* at the
North West University

Supervisor: Dr JT Janse van Rensburg

Co-supervisor: Mr JJ Greeff

Graduation ceremony: December 2020

Student number: 23211164

DECLARATION: AUTHENTIC SUBMISSION

I, Ian Loyiso Ngqoyiyana, declare that

Developing an artefact for raising social engineering awareness among administrative staff

is my own work and that all the sources I have used or quoted have indicated and acknowledged by means of complete references, and this dissertation has not previously been submitted by me for a degree at any other university.

Signature:

Date: August 2020

DECLARATION: LANGUAGE PRACTITIONER

To whom it may concern

Cecile van Zyl
Language editing and translation
Cell: 072 389 3450
Email: Cecile.vanZyl@nwu.ac.za

Dear Mr / Ms

Re: Language editing of dissertation: Developing an artefact for raising social engineering awareness among administrative staff

I hereby declare that I language edited the above-mentioned thesis by Mr Ian Ngqoyiyana (student number: 23211164).

Please feel free to contact me should you have any enquiries.

Kind regards

Cecile van Zyl
Language practitioner
BA (PU for CHE); BA honours (NWU); MA (NWU)
SATI number: 1002391

ACKNOWLEDGEMENTS

I would like to sincerely thank the following people:

- To my supervisor, Dr. J.T. Janse van Rensburg, your patience and diligence is like none other – thank you for taking me under your wing and guiding me through this study.
- To my co-supervisor, Japie Greeff, thank you for being a part of this study, your input has been invaluable.
- To the participants and experts who availed themselves for this study.
- To my parents, Alfred Mbuyeleli and Gladys Kebitsamang, thank you for supporting me throughout my academic journey.
- And to my wife, Jesseca, thank you for putting up with the late nights and supporting me through thick and thin.

ABSTRACT

Social engineering is one of the biggest cyber-security threats faced by organisations. Cyber-criminals no longer primarily aim to exploit information systems, but rather target the 'low hanging fruit', which is the human element. End-users, primarily administrative staff, are at the highest risk of these social engineering attacks. Administrative staff such as secretaries, clerks, receptionists, etc. have access to sensitive information about the organisation. These administrative staff are considered to be easy targets for attackers, especially in advanced persistent threat (APT) attacks. Administrative staff are less likely able to quickly spot social engineering attack cues, as they are not trained to constantly deal with such attacks. It is for this reason that an intervention is required to raise awareness on social engineering attacks.

This study seeks to develop an artefact that is suitable to raise awareness of social engineering attacks on users who are employed as administrative staff in medium to large organisations, specifically within the context of South Africa. Revision of the literature indicates that limited research has been performed regarding interventions to raise social engineering awareness for administrative users who are employed in medium to large organisations in Southern Africa.

The research findings indicate that game-based artefacts can be used to raise awareness about social engineering issues.

Research paradigms are discussed as part of the literature review. Design science research (DSR) is a useful approach to developing and reporting on artefact creation. The research is structured according to the design science research methodology (DSRM) process model by Peffers *et al.* (2007:54) and the artefact development process is guided by the DSR cycles by Hevner (2007:2). This DSR study is reported on similar to the approach followed by Mckenney and van den Akker (2005:49).

Cyber security is discussed as part of the literature review. The cyber-security issues are discussed covering concepts of cyber-crime, cyber-terrorism, and cyber-warfare. The cyber-security issue extensively discussed is cyber-crime, with a key focus on the types of cyber-crimes and social engineering being the focal point for the cyber-crimes discussion. The types of social engineering attacks are discussed which lead into a discussion on the interventions available for raising awareness regarding cyber-security issues.

The interventions for raising cyber-security awareness (which include social engineering awareness interventions) are identified from the literature and presented in a participatory design workshop to participants who form part of the target user group (which are administrative staff

employed in medium to large organisations). Game-based artefacts are identified, with the participants, to be the preferred artefacts to address the social engineering awareness issue. The game-based artefact is initially developed as a conceptual design and iteratively improved into a usable prototype. The design requirements are gathered from the target users, translated into functional and actionable design inputs, and implemented and continuously reviewed by the design experts from academia. The game-based artefact is developed through multiple iterations and participatory design workshops. It is then evaluated through a summative evaluation and testing approach to determine its reaction and learning evaluation. The reaction evaluation seeks to determine whether the artefact is suitably designed according to the design requirements gathered throughout the design and development processes. The learning evaluation seeks to determine whether the artefact can be used to bring about a learning experience in the users. It is also tested for quality to determine whether it addresses the quality criteria of a DSR artefact. The quality evaluation criteria addresses the validity, practicality, and impact potential of the game-based artefact.

Due to the COVID-19 pandemic, the summative evaluation and testing (reaction and learning evaluation) is not performed as a participatory design workshop – electronic forms are provided to the participants instead. Two groups of participants are involved in the design, development, and evaluation of the artefact. Participatory design workshops are used to gather the design and development information. In the participatory design workshops, questions are asked about the design of the artefact and the feedback received is electronically captured and analysed using open-coding to identify themes in the data. The first group of participants are from an academic (academia) institution and are mainly involved in the design and development of the artefact. The first group includes the target users (participants) as well as the research experts (which include the DSR experts and design artist). The second group of participants are from a medium to large organisation (industry). The second group of participants include the target users (participants) as well as the cyber security expert. The second group of participants (from industry) are mainly involved in the evaluation of the artefact with a small subset also being involved in the design and development process. In total, 27 participants are involved in this study. The participants from both academia and industry are randomly sampled based on their availability. Twelve of the 27 participants are involved in the design and development of the artefact, and are from different roles from both organisations (academia and industry). The design and development of the artefact occur over three participatory design workshops. Workshops 1 and 2 are performed with a total of eight participants from the first organisation (academia) for the development of the conceptual and first prototypes. The third workshop is performed with the participants from the second organisation (industry) in the development of the second prototype. Four of the 12 participants involved in the design and development also provide feedback on the reaction

evaluation of the artefact. The remaining 15 participants from organisation two (industry) are employed in administrative or similar roles and are involved in the learning evaluation of the artefact. Both evaluations are electronically presented to the participants using electronic forms. The reaction evaluation form contains open-ended questionnaires with the results being analysed through open-coding to identify themes in the data. The learning evaluation form contains a pre- and post-test questionnaire, with the results being quantitatively compared to determine whether a learning experience has taken place on the participants after having played the game-based artefact.

The study results indicate that web-based artefacts are more preferred for a digitally connected society that prefers to be able to access resources from any location. This has proven relevant during the COVID-19 pandemic, where social distancing was crucial. Video tutorials are a suitable avenue for providing social engineering information during gameplay.

The tools used to develop the artefact were also useful. These tools included Image Map, Cloudflare, Apache 2.4.43, GoDaddy, Google Forms, Microsoft Azure, Twine 1.4.2, Unity 2019.1.14, Microsoft OneNote, Microsoft Word, Microsoft PowerPoint, NaturalReader, HTML, Javascript, Blender 2.25, LetsEncrypt (CertBot), and Linux Ubuntu 18.04. These tools are discussed in the study.

Keywords: Cyber-security, social engineering, design science research, participatory design, research paradigms, learning evaluation, administrative staff, and reaction evaluation

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION AND BACKGROUND TO THE STUDY

1.1 Introduction and background

Kshetri (2019:77) identifies Africa as becoming one of the continents that is highest at risk of cyber-attacks. This is mainly due to vulnerable systems, lax cybersecurity practices, lack of budget, weak legislation and law enforcement, and most importantly, lack of skills and awareness among end-users. Organisations are investing large amounts of money on technology-based information security solutions to defend their information system assets from cyber-attacks (Biancotti, 2017:5). However, even state-of-the-art technologies available on the market are not able to defend systems against all modes of penetration from an attacker, simply because information security is only as strong as its weakest link – the human factor. The human element is exploited by attackers through a technique that abuses the flaws in human logic (cognitive biases) in an attack that is known as social engineering (Gallegos-Segovia *et al.*, 2017:2). Mouton *et al.* (2016:187) as well as van Heerden *et al.* (2018:2) identify the human element as being the first point of attack, which is often the weakest element that cyber criminals target in order to successfully exploit an organisation's systems. The best defence against these social engineering attacks is to raise awareness about them. This study seeks to do just that – to develop an artefact that can be used to raise social engineering awareness within organisations, particularly amongst administrative staff, who are identified to be the most vulnerable targets of these attacks.

The term *cyber* has become a buzzword that has grabbed the attention of many organisations in the 21st century. The Oxford English Dictionary (2001) defines cyber as anything "*relating to, or involving computers or computer networks (such as the Internet)*". This era of interconnectivity brings about new and improved ways to communicate and do business. This era also brings the element of cyber-crime. Although there is no conclusive definition, cyber-crime is defined as any criminal activity that uses computers or the Internet (Mendoza, 2017:2). This crime is performed by cyber-attackers who intend to steal or interrupt the flow of information that is being transmitted. Cyber-crime can occur in many different ways, ranging from identity theft, denial of service (DoS) attacks, theft of intellectual property, or Internet fraud (Whitson, 2019). Cyber security is the measure taken to protect hardware, software, or sensitive information against unauthorised access or damage.

Within the context of computer and information security, social engineering is a combination of techniques that are used against a victim to convince them to divulge confidential information or to perform actions that could compromise the security of an organisation's information assets (Hatfield, 2018:102). Furthermore, social engineering attacks are categorised into two types of

intrusions, either human-based or technology-based (Xiangyu *et al.*, 2017:26). Human-based intrusions occur when the attacker interacts with the actual human victim through media such as telephone calls, physical interactions, etc. Technology-based attacks occur when the human victim is exploited purely through technological interactions (no interaction happening between victim and attacker), such as those through e-mails, website pop-ups, etc.

The human factor is an oversight that is often neglected by management in organisations, which consequently contributes to significant security breaches. Aldawood and Skinner (2018:62) place emphasis on humans being one of the weakest links within an organisation's cyber security strength. They go on further to discuss that cyber-criminals no longer aim to exploit information systems, but rather target the 'low hanging fruit', which are humans within the organisation. All employees need to be aware of social engineering attacks (Aldawood & Skinner, 2018:64). However, users who most often have access to sensitive information or systems are in administrative positions.

This study seeks to determine a suitable approach to raise awareness of social engineering attacks for users who are employed as administrative staff in medium to large organisations, specifically within the context of South Africa. Limited research is available regarding interventions to raise cyber security awareness within South Africa. None of the research is, however, directed specifically at administrative users who are employed in medium to large organisations within Southern Africa. This, therefore, indicated a research gap for research within the identified context.

Section 1.2 of this chapter discusses the concepts that are key to the study. It covers the aspects of cyber security, briefly discussing what the concept entails, the trends observed that are specific to the context of this study, the common attack vectors within this context, and lastly, the concept within cyber-security that is relevant to this study. This section also discusses the aspects of social engineering as the cyber-attack vector that is pertinent to this study, as well as the chosen methodology to conduct this research, which is design science research.

Section 1.3 discusses the research problem and provides context to the study. This understanding leads to the identification of a research gap that paves the way for this study to be performed. The research questions are further discussed. These questions are divided into the primary and secondary objectives. The objectives are used to determine whether the research questions are answered at the end of the study.

Section 1.4 describes the research methodology that is followed throughout the study. It provides an overview of the methodology used to design, develop, and evaluate the artefact, and also

describes the process that is used to report on the design, development, and evaluation of the artefact. The participants used to gather data in the study are discussed, including the methods used for the analysis of the data. Ethical considerations that are relevant for conducting this research are discussed with the study delimitations.

The chapter layout for this study is expanded on in Section 1.5. It gives context to the chapters that follow further in the study. Section 1.6 concludes this chapter.

1.2 Central concepts

This section creates a shared understanding of the concepts central to the study, which are cyber-security, social engineering, and design science research.

1.2.1 Cyber-security

Cyber-security is a concept that has gained different meanings over the years. Terms that are regularly used within this context are computer security, IT security, or information security. Schatz *et al.* (2017:66) describe cyber-security as the approach and actions, with the associated risk management processes, that seek to protect the confidentiality, integrity, and availability of assets and data. This definition is supported in a study by von Solms and von Solms (2018:5), who define cyber security as the “preservation of the confidentiality, integrity and availability of information in Cyberspace”. There are a variety of constantly changing attack vectors that cyber security aims to prevent. The scales of the attack vectors are commonly executed as cyber-crime, cyber-warfare, or cyber-terrorism.

A study by van Niekerk (2017:122), which analyses the number cyber-incidents that occurred in South Africa between 1994 and 2016 (Figure 1-1), indicates that cyber-attacks are on the rise in South Africa.

Stiawan *et al.* (2017:127) identify six techniques commonly used by threat actors to gain access to a system; these methods include web implants, malware (viruses), SQL injections, phishing, password guessing attacks, as well as flooding attacks (denial of service (DoS) attacks). Social engineering is an attack vector that is often overlooked. Users of information systems are seen as the weakest link for cyber-attackers to gain access to information systems (Heartfield & Loukas, 2015:1). Mouton *et al.* (2016:187) support this view by stating that the human element is the first point of attack and is often the weakest element that cyber-criminals target in order to exploit systems. What makes social engineering attacks powerful and effective is that they are not easily preventable using hardware and software solutions – as long as the human element is not trained to identify and prevent these attacks (Fatima & Naima, 2019:1).

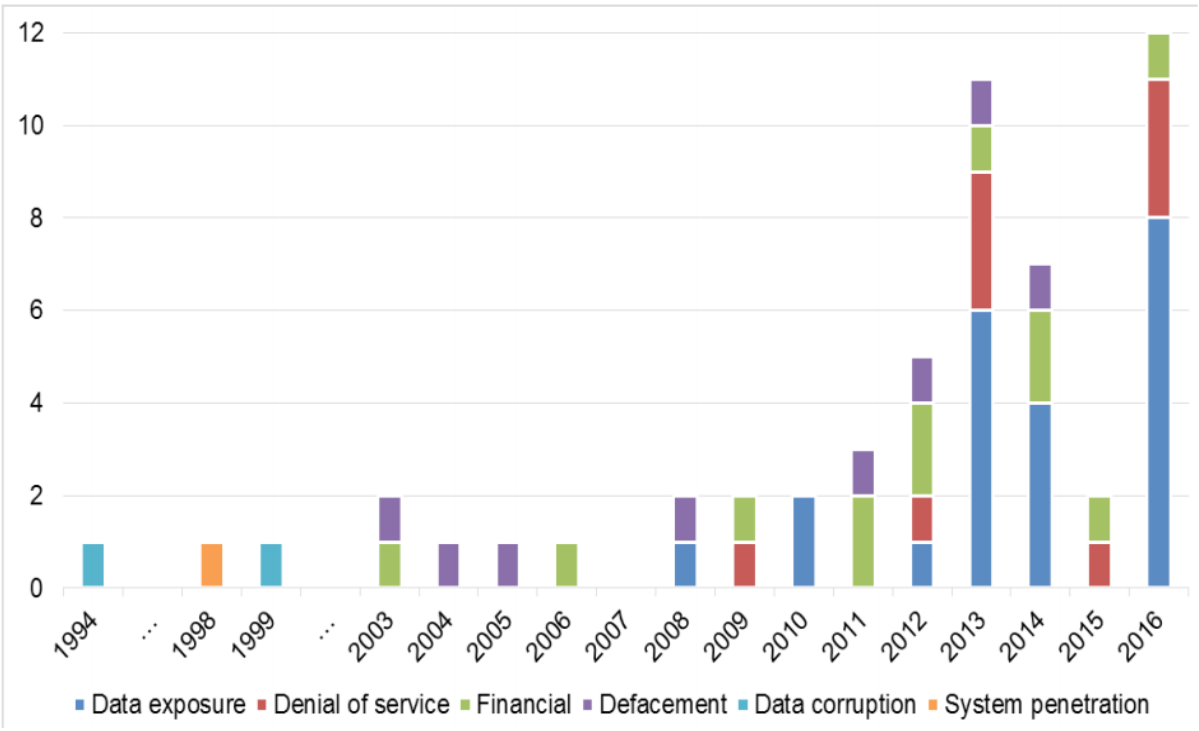


Figure 1-1: Trend of instances against cyber impact types that occurred in South Africa between April 1994 and the year-end of 2016 (van Niekerk, 2017:122)

Pfleeger *et al.* (2014:489) mention that users of information systems within organisations are the weakest link in cyber security. Green and Smith (2016:2) however, argue that system administrators and developers are susceptible to making system configuration mistakes and are as a results of this, also vulnerable to social engineering attacks. This could pose a greater risk to the organisation than that presented by the end-user.

For the purpose of this study, the focus of social engineering is on the end-users, specifically users within medium to large organisation who are employed in administrative roles such as receptionists, secretaries, personal assistants, etc. The primary reason for focusing on end-users who are employed in administrative roles is because these users have access to sensitive information that, if obtained by an attacker, could be used to perform other more targeted attacks at users who have privileged access.

1.2.2 Social engineering

Social engineering is a concept within cyber security that deals with cyber-attacks on people (Parthy & Rajendran, 2019:1). It is an attack vector that exploits the various psychological

weaknesses of a human victim in order to gain access to hardware and other sensitive information (Pozo *et al.*, 2018:108).

Social engineering is the easiest and most preferred attack vector in cyber security. This is primarily because the attacks can be performed in a relatively short space of time and do not require extensive technical expertise. A study conducted by Krombholz *et al.* (2015:113) on advanced social engineering attacks identifies social engineering as an emerging serious threat to virtual communities that has become an effective means that is used by attackers to gain access to information systems. Social engineering is affecting companies at a global scale due to the nature and complexity of the communication technologies available on the market, as well as the tools that are available and being used by the end users. These attacks are usually carried out in four major phases (Figure 1-2), which are: (1) information gathering, (2) gaining the victim's trust, (3) exploitation, and (4) exit (Parthy & Rajendran, 2019:1). During the *information gathering* phase, an attacker gathers background information about the target. This information is used to identify the victim's weakness and to tailor the attack in such a way that it convinces the victim to divulge sensitive information or unknowingly perform malicious actions. At the *gaining trust* phase, the attacker gains the victim's trust while keeping the victim's weakness in mind. The victim is then convinced to divulge the sensitive information. The attacker will use the divulged information to *exploit* the targeted enterprise. Once the attacker has accomplished his objective, all traces of the attack's digital footprint are erased.

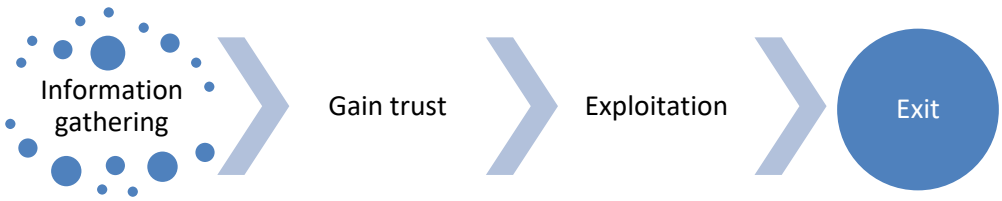


Figure 1-2: The four phases of a social engineering attack (Parthy & Rajendran, 2019:1)

Within the South African context, a limited amount of social engineering awareness research has been done, such as the study by Kritzinger (2017:20) on *growing a cyber-safety culture amongst school learners in South Africa through gaming*, which examines a platform to raise cyber-awareness among school children, but does not cover the demographic of the working class. Jansson and Von Solms (2011:30) present a solution in the form of a step-by-step flowchart that employees can follow to identify, mitigate, or even prevent a potential social engineering attack, but conclude that it requires extensive further testing in practice. Similarly, Jansson and von Solms (2013:584) conducted a study titled *Phishing for phishing awareness* that simulates a phishing attack on a focus group of subjects. The simulation is followed by an awareness

campaign, and a phishing attack is conducted again to determine whether the awareness campaign had raised awareness on the subjects.

The focus of this study is on designing an appropriate artefact that can be used to raise social engineering awareness among administrative staff. Design science research is therefore the preferred research methodology, as its key focus is on producing unique artefacts that can be evaluated for their effectiveness.

1.2.3 Design science research

Design science research is a set of analytical techniques and views that are used when performing research within the field of information systems. It is an information systems research paradigm that seeks to improve and understand the various aspects of information systems through the production of unique artefacts, which are then analysed and measured for performance (Vaishnavi *et al.*, 2004/2019:1). This view is supported by Hevner *et al.* (2004:75), who describe design science research as a paradigm that "*seeks to extend the boundaries of human and organisational capabilities by creating new and innovative artefacts*". Hevner (2007:2) encapsulates the design science research process into three cycles, namely the *relevance*, *rigor*, and *design* cycles.

Peffers *et al.* (2007:54) describe six activities (Figure 1-3) to performing a design science research study, which are: (1) problem identification and motivation, (2) objectives of a solution, (3) design and development, (4) demonstration, (5) evaluation, and (6) communication.

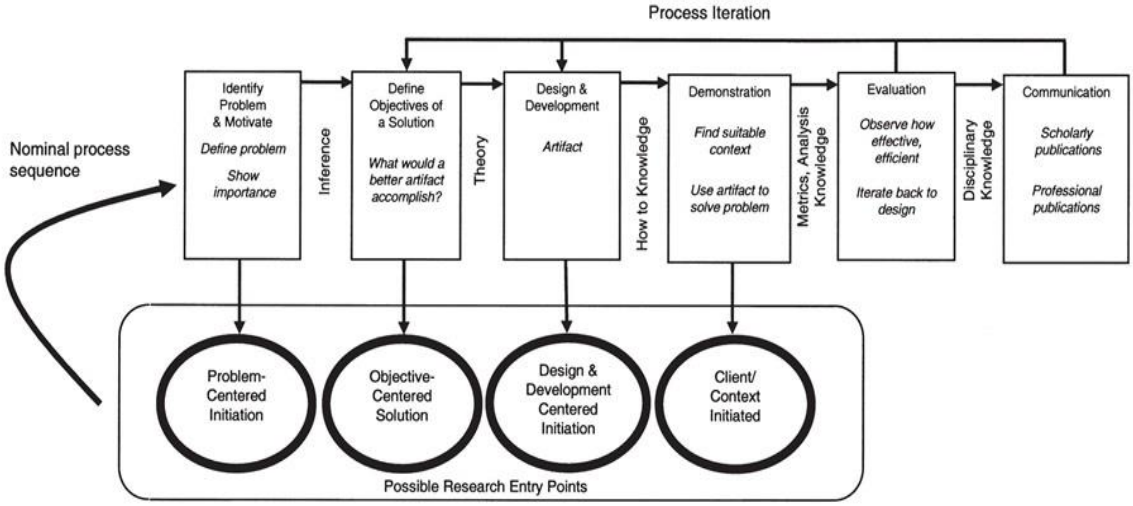


Figure 1-3: Design science research methodology (DSRM) process model (Peffers *et al.*, 2007:54)

The DSRM process model as it relates to this study is explained.

1. **Problem identification and motivation:** A research problem is identified within the field of information systems. The problem is that administrative employees within medium to large organisations lack awareness regarding social engineering issues. The research problem is discussed in Section 1.3;

2. **Objectives of a solution:** The objective of the study is to raise awareness regarding social engineering issues among administrative staff employed in medium to large organisations. The objectives are discussed in Section 1.3;

3. **Design and development:** An artefact is designed and developed using the process defined in the DSR cycles by Hevner (2007:2). The requirements are gathered from the participants and the artefact is developed using tools that are suited to cater to the requirements. The design and development process of the artefact is described in Chapter 5 and Chapter 6;

4. **Demonstration:** The artefact developed is continuously field tested as a means of contextualising it to the problem it needs to address;

5. **Evaluation:** The artefact is evaluated in Chapter 7 (as a summative evaluation and test) to determine whether it addresses the research problem;

6. **Communication:** Findings are communicated as contributions to the information systems research knowledge base. This is communicated in Chapter 8, the conclusion of this study.

These research steps are supported by Baskerville *et al.* (2015:543), who indicate that a design science research study will typically be composed of four aspects, namely: (1) a design-science research project, (2) the design and development of an artefact (build and evaluate), (3) the production of new knowledge from the design and development process, and (4) the creation of reports or articles describing the design science research project.

1.3 Research problem and objectives

The aim of this study is discussed in this section. Section 1.3.1 discusses the research problem and research questions. The objectives of this study are further discussed in Section 1.3.2.

1.3.1 Research problem

Research by van Niekerk (2017:113) , Kritzinger (2017:16), Warwick (2016), Krombholz *et al.* (2015:113), Heartfield and Loukas (2015:1), as well as other prominent authors, indicate that social engineering is one of the biggest cyber security threats faced by organisations. Organisations spend vast amounts of money in an attempt to secure their information systems, but often neglect the end-user. End-users are at the highest risk of these social engineering attacks (Furnell & Vasileiou, 2017:5). Administrative staff are end-users who often have access to sensitive internal business information and processes. The combination of being an end-user neglected by the information security function, and having access to sensitive information makes administrative staff prime targets for cyber criminals. It is for this reason that an intervention is required to raise awareness on social engineering issues towards administrative staff who are employed in medium to large organisations.

Research on interventions that are suited for administrative employees is not adequately catered for. It is therefore the purpose of this study to design an artefact that will cater specifically for administrative staff. The studies pertaining to social engineering and raising awareness for administrative staff are limited within the context of South Africa, and therefore there is a gap in this research field.

Within the South African context, this research is particularly crucial in that social engineering attacks have grown and become more prominent and successful avenues for hackers to compromise the information systems of organisations (van Heerden *et al.*, 2018:2).

In order to understand the research problem, the following research questions are posed:

- Which type of artefact is suitable to raise social engineering awareness among administrative staff?
- How can an artefact be designed in a way that it can meet user acceptance requirements to raise awareness on social engineering?
- How can design science research be used to design an artefact to raise social engineering awareness among administrative staff?

1.3.2 Objectives of the study

1.3.2.1 Primary objective

The primary objective of this study is to design and develop an artefact that can be used to raise awareness about social engineering attacks among administrative staff in medium to large organisations.

1.3.2.2 Secondary objectives

The secondary objectives of this study are tabulated in Table 1-1. In order to facilitate the phases of the DSR framework, it makes sense to structure the theoretical objectives according the phases of the DSR process. The secondary objectives are therefore organised according to the design science research methodology (DSRM) process model phases by (Peffers *et al.*, 2007:54), which were depicted in Figure 1-3 of Section 1.2.3.

Table 1-1: Secondary objectives of the study organised according to the DSRM process model by (Peffers *et al.*, 2007:54)

DSR process	Objectives
Problem identification and motivation	**Theoretical objectives** • To identify the research problem. • To motivate the process for conducting the research. • To determine the required fields of research to inform a solution for the research problem.
Objectives of a solution	**Theoretical objectives** • To create a shared understanding of design science research. • To understand the concepts of cyber-security and the area of social engineering within cyber-security. • To identify what artefacts are available to raise cyber-security and social engineering awareness in particular.

DSR process	Objectives
	Empirical objectives • Present findings from the literature in a participatory design workshop. • Analyse the feedback received from the requirements gathered during the participatory design workshops. • Develop and present a conceptual design as a solution to the problem that is based on the requirements gathered from the target users.
Design and development	**Theoretical objective** • To form a conceptual link between design science research and the feedback analysed from the data obtained during the requirements analysis.
	Empirical objectives • To design and develop an artefact that meets the design and functionality requirements obtained from the requirements analysis. • To develop the artefact through an iterative approach until a usable prototype is reached.
Demonstration	**Theoretical objectives** • To explain how the requirements analysis and literature informed the design process through the use of artefact screenshots coupled with explanations
	Empirical objectives • To demonstrate the artefact to the target audience. • To continuously evaluate the results obtained from the iterative demonstration of the artefact and determine any notable responses for future research at the end of the development prototype.
Evaluation	**Theoretical objective** • To determine a suitable reporting method for the feedback received from the summative evaluation and testing of the artefact.
	Empirical objectives • To conduct a reaction evaluation with participants from the target audience as part of the evaluation of the artefact. • To conduct a learning evaluation with participants from the target audience as part of the evaluation of the artefact. • To analyse the feedback obtained from the reaction evaluation using qualitative data analysis techniques. • To analyse the feedback obtained from the learning evaluation using quantitative data analysis techniques. • To evaluate the quality of the artefact against a quality evaluation criteria.

DSR process	Objectives
Communication	**Theoretical objectives** • To communicate the design science research approach followed developing an artefact for raising social engineering awareness among administrative staff. • To communicate limitations within the context of the study by reflecting on restrictions of the research. • To communicate the reflections on the study recommendations for further improvement of the artefact in future research.

1.4 Research methodology

This section outlines the research methodology that is followed in this study. It outlines the motives for selecting the participants who are used and also provides an outline of the approach taken to gather and analyse data. Ethical considerations to conduct this study are also outlined, including the study's delimitations.

1.4.1 Overview

The research methodology chosen for this particular study is design science research. The problem and purpose of this study require the design of an artefact that would solve a real-world problem (Hevner *et al.*, 2004:76). Design science research provides a process that allows for the design of unique and useful artefacts, and it is therefore for this particular reason that this research methodology is chosen.

The research process for this study follows the DSRM process model by Peffers *et al.* (2007:54) (Figure 1-3). To facilitate the design of the artefact, the cyclical approach for design science research by Hevner (2007:2) is used (Figure 1-4).

The artefact design follows a cyclical and iterative process that requires the design of the artefact to be rooted in a research methodology that supports this approach.

The reporting of the process that is followed throughout the design and development of the artefact follows the cyclical process, similar to the process followed by Mckenney and van den Akker (2005:49) in the evaluation of the CASCADE-SEA program (Figure 1-5). This reporting process is explained in Chapter 2, Section 2.4.4.

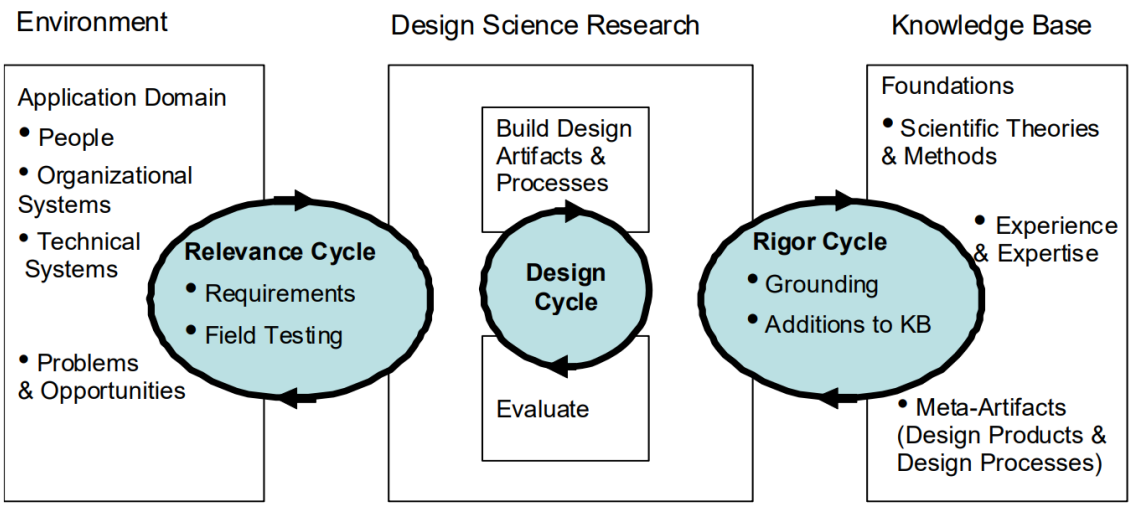


Figure 1-4: The design science research cycles (Hevner, 2007:2)

Before the design of the artefact, a needs analysis is performed to determine the gap for performing the research, as well as to determine the specifications that meet a suitable design. A prototype design is developed through a collaborative effort between the participants as well as the design science research experts. A final working artefact is the result of the iterative design, development, and formative evaluation process. The artefact is then evaluated with a new group of participants. The final evaluation process is imperative to determine whether the artefact addresses the research objectives. The summative evaluation consists of the final evaluation and query, as well as the quality criteria review.

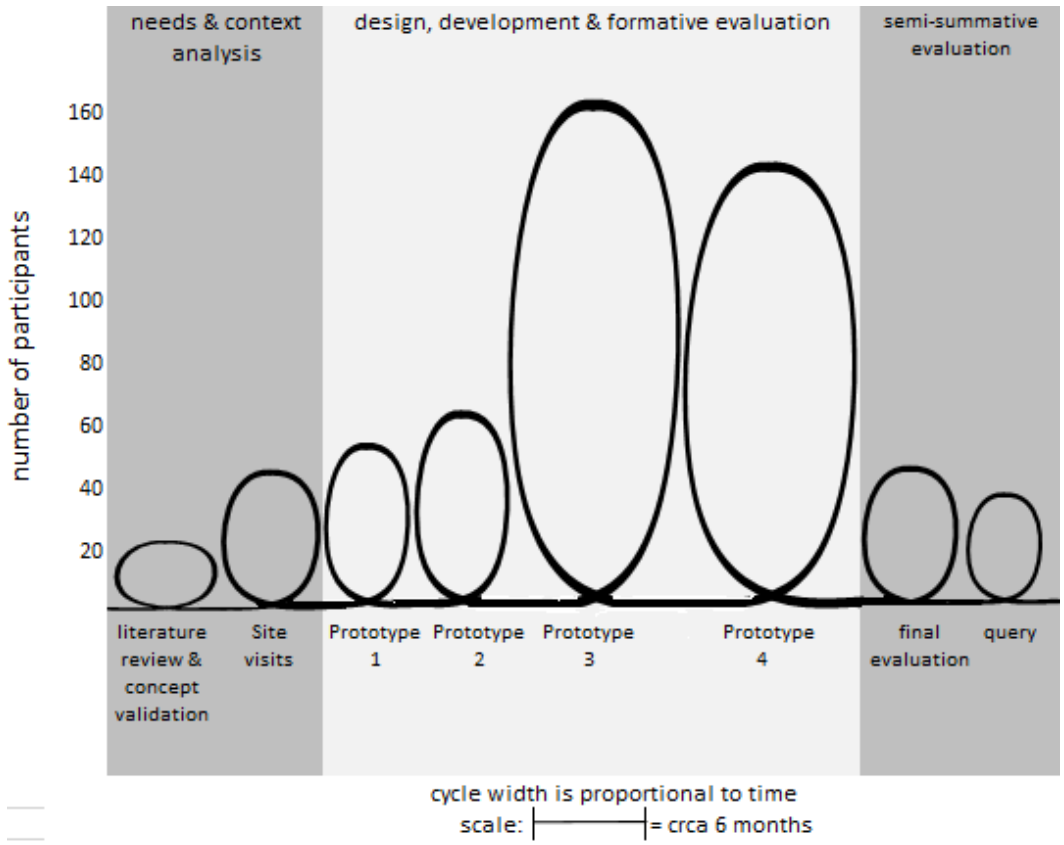


Figure 1-5: An example of the cyclical approach to the three phases followed in the evaluation of the CASCADE-SEA program (Mckenney & van den Akker, 2005:49)

1.4.2 Participants

This research focuses on participants who are identified to be most susceptible to social engineering attacks. The participants mainly fall within the demographic of end-users employed in administrative roles within a medium to large organisation. These participants are selected particularly because they have access to sensitive information within the organisation. The sensitive information is information such as finances and internal contacts. In many instances, these delegates approve workflows within business critical systems, which consequently means that there is a greater risk to organisations resonating from these employees.

Even though this research study is primarily focused on end-users employed in administrative roles within a medium to large organisation (which we will refer to as the target user participants), it is imperative to note that research experts from academia, a design artist, as well as a cyber-security expert and cyber-security professionals were involved in the study as participants.

The experts are consulted to inform the design of the artefact and also make up the participants involved in the design and evaluation of the artefact. These experts include design science research, cyber-security, game design, and user experience experts. These experts form an integral and supportive function in guiding the process of designing and developing a usable artefact.

The participants specifically used throughout this study are administrative staff from medium to large organisations, selected from a university (also referred to as Company A in this study) and a company from industry (also referred to as Company B in this study). The participants who provide data range from four (4) to six (6) per workshop session. The results from these data gathering workshops are discussed throughout Chapters 5 to 7. Chapter 4 discusses the approach that will be used in designing, developing, and evaluating the artefact.

1.4.3 Data gathering and analysis

Qualitative data is iteratively gathered from the participants in three participatory design workshops to obtain requirements and feedback regarding the design of the artefact. The results gathered in the participatory design workshops are analysed using open coding to identify themes in the data. Open coding is a qualitative analysis technique where units of data are labelled through concepts and themes which were identified in the data. These themes do not come from existing literature or theories (Hoepfl, 1997:55). The themes are then used to iteratively develop and improve the game-based artefact.

A summative evaluation and test (discussed in Section 7.3) is performed to test the game-based artefact through the ***learning*** evaluation and ***reaction*** evaluation levels as per the four-level evaluation model by Petri and von Wangenheim (2016:995) (discussed in Section 2.4.2). The final summative evaluation and testing was intended to happen as two additional workshops (as workshops 4 and 5), however, due to the COVID-19 pandemic, the questionnaires are delivered to the respective participants using Google forms as an online delivery platform. The ***reaction*** level evaluation (discussed in Section 7.3.1) is an open-ended questionnaire (depicted in Appendix O) that aims to determine from the participants whether the design requirements were adequately translated into the working prototype. The results are also analysed using open-coding to identify themes in the coded data. The ***learning*** level evaluation (discussed in Section 7.3.2) is a pre- and post-test questionnaire (depicted in Appendix M and N) that aims to determine whether the game-based artefact has brought about a learning experience in the participants. These learning level evaluation questionnaire's questions pertain to social engineering and are initially presented to the participants (as a pre-test questionnaire) to rate their initial awareness of social engineering issues. The participants then interact with the game-based artefact and are

presented with an additional set of questions (as a post-test questionnaire). Pre- and post-test scores are evaluated and compared to determine whether any learning took place (see Section 7.3.2 for results).

1.4.4 Ethical considerations

A code of conduct, as prescribed by the North-West University, was signed by the researcher (refer to Appendix A). The code of conduct commits to the four principles of research integrity, which are honesty, accountability, good stewardship, as well as professional courtesy.

Ethical clearance for conducting research was obtained from the North-West University through the ethical clearance application process. The application was submitted to the ethics subcommittee of the faculty who reviewed the application for risk. The application was approved for the study and an ethics number NWU-001177-19-S9 was awarded (refer to Appendix B).

The ethical principles for design science research, as described by Myers and Venable (2014:806), are adhered to in this study. The ethical principles include informed consent, privacy, honesty and accuracy, as well as quality of the artefact. These are discussed in further detail in Chapter 2, Section 2.4.5.

1.4.5 Delimitations

The delimitations that are identified for this study are as follows:

- Staff employed in administrative roles within medium to large organisations are specifically chosen as they are identified to be the end-users who have access to sensitive information and are also most susceptible to social engineering attacks.
- Social engineering is chosen as the primary cyber-security attack vector, because research has shown that social engineering is the most preferred attack vector used by cyber-criminals, as it is effective and does not require any specialised skills to successfully exploit people, and as a result, the critical business systems.

1.5 Chapter layout

The layout of this study is structured as follows:

Chapter 1: Introduction and background to the study

This chapter provides background to the study by describing the motive for performing the research, defining the objectives the study aims to address, and also describing the key concepts that are central to the study. The research methodology that guides the study is also presented.

Chapter 2: Research methodology

Chapter 2 provides a general understanding of the positivist, interpretivist, critical social theory, and design science research paradigms with a key focus on the ontological and epistemological assumptions, as well as the methodology of each. The data gathering methods are discussed, followed by a detailed explanation of design science research as the appropriate paradigm of the study. The section ends with an explanation of how the study is positioned.

Chapter 3: Literature review

A broad discussion on cyber-security and the most commonly used cyber-attack vectors in cyber-crime is provided in this chapter. It goes on to give a special focus to social engineering by describing the different attack vectors and the interventions that have been developed by researchers to raise awareness regarding these attacks. This section concludes with an overview of the artefacts that can be used to raise social engineering awareness.

Chapter 4: The DSR approach followed in this study

Chapter 4 provides deeper insight into how the artefact's design and development process is rooted in design science research. The reporting approach for the design, development, and evaluation of the artefact is also discussed in this chapter. It describes how the artefact would undergo pre-, mid-, and post-developmental phases. These phases are respectively indicative of the activities that occur before the actual artefact is developed (pre-artefact), when the actual artefact is developed (mid-artefact), and the activities that occur after the artefact had been developed (post-artefact).

Chapter 5: Pre-artefact

Chapter 5 describes the activities that take place throughout the design of a conceptual artefact. This chapter relates to the needs and context analysis phase of the reporting approach. The product of this chapter is to produce a conceptual artefact that is validated by the target user group. The conceptual artefact guides the design of the first prototype, the design of which is described in Chapter 6.

Chapter 6: Mid-artefact [prototype 1 & prototype 2]

Chapter 6 describes the activities for the development of the first and second prototype artefact. The artefact design and development is guided by the requirements that are gathered from the conceptual artefact, as described in Chapter 5. Design science research experts also provide guidance on how the prototype artefact is designed. This chapter aligns with the design, development, and formative evaluation phases of the reporting approach, as described by Mckenney and van den Akker (2005:49).

Chapter 7: Post-artefact

Chapter 7 describes the activities of the summative evaluation and testing of the second prototype. This chapter aligns with the summative evaluation and testing of our reporting approach as described in Section 2.5.2. The game-based artefact is evaluated in the summative evaluation and testing as a reaction evaluation, learning evaluation, and quality evaluation. The reaction evaluation seeks to determine how the participants feel about the artefact, the learning evaluation seeks to determine whether the artefact has brought about a learning experience in the participants, and the quality evaluation seeks to determine whether the artefact has been design according to a predefined quality criteria.

Chapter 8: Conclusion

This chapter concludes the study by discussing how the primary and secondary research objectives set out in Section 1.3.2 were addressed (in Section 8.2). It also discusses the artefact development and evaluation process in Section 8.3 and further discusses the DSR checklist, as it relates to this study, to determine whether it adequately satisfies the requirements of a DSR study. The study limitations that prevented certain research aspects from being performed as well as potential future work for other research studies are summarised in Section 8.5. The section then closes with the researcher's reflection on the study, as well as any other concluding thoughts.

1.6 Conclusion

This chapter has provided an overview of the study by discussing its purpose. The concepts central to the study were generally described. These concepts related to cyber-security, social engineering, and design science research. The general cyber-security issues were described, including the attack vectors and how they relate to the context of this study. The research problem and objectives were also discussed. The research problem relates to an ongoing concern in cyber security, specifically within the context of South Africa where cyber-attacks are found to be targeted at end-users, primarily through social engineering attacks. The targeted users were

identified to be administrative users employed in medium to large organisations. The research problem informed the primary objective, which was to design and develop an artefact that can be used to raise awareness about social engineering attacks among administrative staff in medium to large organisations. The secondary objectives, which support the primary objectives, were also discussed. This study was structured according to the six activities of the DSRM process model by Peffers *et al.* (2007:55), and as a result, the theoretical and empirical objectives for the secondary objectives were organised according to these six activities.

This chapter also discussed the research methodology that will be followed in the design, development, evaluation, and reporting of the artefact. The development of the artefact was grounded in design science research cycles by Hevner (2007:2), and was reported in alignment with the process that is followed by Mckenney and van den Akker (2005:49). The participants, ethical considerations, and study delimitations were also discussed.

The chapter that follows will provide an overview of four research paradigms, namely positivism, interpretivism, critical social theory, and design science research. The ontological and epistemological assumptions of each of the paradigms will also briefly be discussed. The section will also describe the methodology for each of the four paradigms. Data gathering methods will also be described, which will provide a description of the differences between primary and secondary data, and the data collection techniques that are used in research. The chapter will lead to an in-depth overview of design science research, which is the research methodology chosen for this study.

CHAPTER 2: RESEARCH METHODOLOGY

2.1 Introduction

The primary objective of this study is to design and develop an artefact that can be used to raise awareness about social engineering attacks among administrative staff in medium to large organisations. This chapter will support this primary objective by creating a shared understanding of design science research, which is a suitable paradigm for artefact creation. It is worth noting that authors such as Myers and Venable (2014:801) and Gregor and Hevner (2013:337) view DSR as a paradigm whereas authors such Baskerville and Pries-Heje (2019:55) do not. For the purpose of this study, DSR is accepted as a research paradigm.

In this section of the study, the different research paradigms and methods employed in the field of information systems research are discussed. A paradigm is a set of assumptions adopted by the professional community that allows for the sharing of similar perceptions and for engaging in shared practices (Hirschheim & Klein, 1989:1201). The philosophical assumptions for each paradigm, which include the epistemological and ontological assumptions, are also discussed. Additionally, the methodologies and the methods applicable to each paradigm are discussed.

Research is generally defined as a set of activities which are carried out in a systematic manner in an effort to find out things that are not known. It seeks to understand, describe, predict, and control a phenomenon through a process of collecting, analysing, and interpreting data (Mackenzie & Knipe, 2006:2). Research methods are the techniques that are employed to conduct research (Walliman, 2011:7). It is important to employ suitable research approaches in order to convince other researchers that the conclusions made have validity and that the knowledge created is soundly based.

Researchers in the field of information systems have a responsibility of furthering knowledge within the discipline of information systems. This research will allow them to improve its productive application to human organisations in order to develop and communicate the obtained knowledge concerning both the management and use of the information (Hevner & Chatterjee, 2010a:10).

A research paradigm is viewed as the fundamental construct to a scientific investigation. A research paradigm is a belief system or world view that guides a researcher's investigation (Krauss, 2005:759). A research paradigm ultimately reflects our beliefs about the world we live in (Guba & Lincoln, 1994:105). In the field of information systems, there are four paradigms often used by researchers, which are positivism, interpretivism, design science research, and critical social theory. Each of these paradigms consists of four components, which are the ontology,

epistemology, methodology, and the methods (Scotland, 2012:9). Table 2-1 provides a brief description of each of the paradigms.

Table 2-1: Research paradigms in the field of information systems

Paradigm	Description
Positivism (scientific)	It is the methods which are studied, described and observed objectively and allows general results to be derivable from observations. There is only a single reality (Krauss, 2005:761).
Interpretivism	The information systems world is interpretable but cannot be specified or reduced to theories. It seeks to understand the world through socially construable human experiences. There are multiple realities.(Krauss, 2005:761).
Design science research	It is a paradigm that aims to create or contribute to new research knowledge within a specific research area. Knowledge is in the form of an instantiation of a design theory and is supported by methods, models, and constructs (Vaishnavi et al., 2004/2019:21).
Critical social theory	It is a paradigm that seeks to reach a deeper understanding of social structures and is a knowledge structure that is based on relations that seek to understand the world from our perspective (Harvey, 1990:1).

The ontological and epistemological assumption form the basis of every paradigm (Scotland, 2012:9). Ontological and epistemological aspects are concerned with the way a person views the world.

Ontology refers to the nature of the reality that is going to be studied, including that which is known about the reality. It is concerned with what constitutes reality, or otherwise asking the question of, *what is*? Ontology is of the assumption that the nature of reality has multiple facets (Bergstedt, 2015:41).

"*Epistemology is concerned with the nature and forms of knowledge, as well as how it is acquired and communicated to other people*" (Cohen *et al.*, 2007:7). According to Krauss (2005:759), epistemology poses the following questions: "*What is the relationship between the knower and what is known? How do we know what we know? What counts as knowledge?*" Epistemology therefore refers to the philosophy of knowledge, and seeks to address the fundamental issues of how we come to know. Epistemologies can be either quantitative or qualitative, which is entirely dependent on the researcher's approach to the study.

Bergstedt (2015:41) and Scotland (2012:9) refer to a methodology as a way in which a researcher will go about practically studying that which they believe can be known, which concerns the what, why, when, from where, and how data is to be collected and analysed. Harvey (1990:4) described a methodology as a point where methodical practice, substantive theory, and epistemological underpinnings are combined when there is an investigation of an instance within the social world.

Methodology is therefore concerned with the way in which data is to be collected and analysed (Scotland, 2012:9). In essence, methodologies are the practices for acquiring knowledge (Krauss, 2005:759).

Method refers to the way in which empirical data is collected and analysed, whether it be in the form of asking questions, conducting observations, or through the process of reading documents. Research methods make "*implicit or explicit assumptions about the nature of the world and of knowledge*" (John, 2001:242). The methods for collecting data can either be qualitative or quantitative and are relevant to all paradigms.

To summarise, Healy and Perry (2000:119) state that: "*ontology is reality, epistemology is the relationship between that reality and the researcher, and methodology is the technique used by the researcher to investigate that reality*".

Table 2-2 below provides a high-level summary of the philosophical assumptions of the four paradigms. The summary table is an adaptation of the one provided in the study by Guba and Lincoln (1994:109), as well as Vaishnavi *et al.* (2004/2019:25).

Table 2-2: Summary of the combined philosophical assumptions of the research paradigms by Guba and Lincoln (1994:109) and the DSR paradigm by Vaishnavi *et al.* (2004/2019:9)

	Positivism	**Critical social theory**	**Interpretivism**	**Design science research**
Ontology	Reality is capable of being understood and is real	The world of the virtual is shaped by gender, cultural, political, economic, ethnic as well as social values which are formed over time	There are many but specific locally constructed realities	There are many contextualised world-states that are socially enabled
Epistemology	It is objectivist and what is found is true	It is subjectivist and whatever is value driven intervention is true	It is subjectivist and what is created is true	It is knowing through making where a controlled construction is created in an iterative manner in order to ultimately reveal meaning

	Positivism	Critical social theory	Interpretivism	Design science research
Methodologies	Relies on experiments or surveys to verify hypothesis primarily through quantitative methods	Relies on dialect to allow changes to occur in the social world where the participants reside	Relies on interpretation or dialect to investigate the world	Relies on development to measure the impact of an artefact on a complex system

The sections that follow will provide more detail on the paradigms defined in Table 2-1, from an ontological, epistemological, and theoretical perspective. The methodology thereof will also be described.

2.2 Research paradigms

2.2.1 Positivism

Positivism is an epistemological stance which suggests that research phenomena can only be examined through scientific methods. It is grounded in the belief that everything is measurable and that if enough is known, the causes and effects of all phenomenon can be revelead (Walliman, 2011:150). "*Positivism strives for objectivity, measurability, predictability, controllability, patterning, the construction of laws and rules of behaviour, and the ascription of causality*" (Cohen *et al.*, 2007:26).

Positivism is the research philosophy that is rooted in the belief that facts and values are distinct and that scientific knowledge only consists of facts (Cohen *et al.*, 2007:11). It originates from the area of thought within a scientific philosophy that is referred to as *logical positivism,* which reflects the perceptions that inform the study of natural phenomena (Al-Khouri, 2007:30).

Positivist research perceives human behaviour and society as a science in the world of the natural sciences. It asserts that phenomena must be segregated and that the observations need to be repeatable. The view primarily serves as a means to test a theory and attempt to develop a measurable understanding of the phenomenon under evaluation. Formal propositions, hypothesis testing, and drawing quantifiable measures of variables from inferences about the phenomenon from a sample size are drawn from a stated population to classify theoretically grounded positivist research (Al-Khouri, 2007:31).

2.2.1.1 Ontological assumptions

Positivism, as explained by Guba and Lincoln (1994:109) and elaborated on by Healy and Perry (2000:119) and Krauss (2005:760), is scientific and assumes that "*science quantitatively measures independent facts about a single apprehensible reality*". It is of the ontological position of realism (also commonly referred to as naive realism) (Guba & Lincoln, 1994:109). Realism is of a perspective that objects have an existence that is disparate from the knower and therefore, concludes that a discoverable reality exists independently of the researcher (Cohen *et al.*, 2007:10). Language provides a representational role of the world and therefore words owe their meaning to objects (Scotland, 2012:10). Positivists believe reality is not negotiated by our senses, but rather through words.

2.2.1.2 Epistemological assumptions

The epistemological assumptions around positivism are that positivism is viewed as a means of obtaining the truth and understanding the world sufficiently such that it can be predictable and controllable. It sees the universe as being deterministic and operated by the laws of cause and effect. Positivism is scientific and empiricist in nature with the idea of observation and measurement being at the forefront of the paradigm (Cohen *et al.*, 2007:10). The investigator and investigated object are seen as independent entities and should not be influenced by one another (Guba & Lincoln, 1994:110). It is imperative to note that within the positivist paradigm, the component parts of a phenomenon are broken apart in order to establish facts. Its key approach is through the scientific method of experimentation that attempts to recognise the laws of nature through direct change and observation (Krauss, 2005:760).

Positivism embraces a four-point doctrine, namely being (Krauss, 2005:761):

1. phenomenalism, which seeks to express that there is only experience that exists and that any other abstractions are rejected;

2. nominalism, which seeks to assert that only linguistic phenomena such as words, abstractions, and generalisations exist, cannot give insight into the world;

3. the segregation of fact from figures; and

4. the consolidation of the scientific method.

Positivism therefore aims to explain and predict phenomena in the world of the social through the determination of regularities and causal relationships between its components.

2.2.1.3 Methodology

The positivist methodology is experimental and manipulative. Questions and hypotheses are stated in propositional form and are verified through empirical tests (Guba & Lincoln, 1994:110). Positivism seeks to explain relationships through the identification of the causes which influence outcomes. It aims to formulate laws for prediction and generalisation by undertaking a deductive approach. Correlation and experimentation are used to reduce the complex interactions and their constituent parts. This is verified and sought through complex direct experience and observation, which primarily involves processes such as empirical testing, random, controlled groups, controlled variable, and sampling. The positivist methodology is viewed as being value neutral and therefore leads the knowledge generated to be value neutral (Scotland, 2012:10). Some of the methodologies employed in the positivist paradigm are experimental, quasi-experimental, correlational, reductionism, theory verification, and normative. Table 2-3 provides a summarised description of the methodologies.

Table 2-3: Some of the research methodologies employed in the positivist paradigm (Scotland, 2012:10)

Name	Description
Experimental	Experimental research is a methodology that is rooted in the scientific practice of physicians and biologists, including other groups of research embodied in the natural sciences, and involves manipulating variables over time, collecting numeric data, and testing causal or correlation models through standardised statistical analysis procedures (Kock et al., 2017:757).
Quasi-experimental	Quasi-experimental research is empirical in nature and is used to estimate the causal impact brought on by an intervention on a target population with random placement.
Correlational	Correlation is a quantitative statistical technique that shows how strong pairs of variables are related. Correlation is determined by rating scales and correlation coefficients.
Reductionism	Reductionism is a philosophical idea that embodies the association between phenomena that can be subdivided into more fundamental phenomena. Reductionism is divided into three parts, namely: Ontological reductionism is a belief that reality is constituted of a minimal number of component; Theory reductionism is the belief that a newer theory does not consume any prior ones, it rather reduces it to its fundamental constituent parts; and Methodological reductionism is a scientific attempt to try and explain sub-components.
Theory verification	A doctrine that states that a preposition is only cognitively meaningful if it can be conclusively determined to be true or false.
Normative	Normative research methodology attempts to not only gather facts about a phenomenon, but also tries to find out which aspects of a phenomenon can be improved.

2.2.2 Interpretivism

In contrast to the positivist paradigm, there exists the interpretive paradigm. It is primarily focused on human interpretations and meanings related to information systems with the perceived and emerging shared creativity of individuals (Al-Khouri, 2007:32). Goede (2004:15) describes interpretivism as an approach that "*focusses on the world of meaning and methods of studying it*".

Interpretivist research seeks to comprehend the phenomena through the accession of meanings that "*participants assign to them as they contend that only through the subjective interpretation of and intervention in reality can that reality be fully understood*" (Al-Khouri, 2007:32). It is therefore accepted that the examination of the phenomenon occur in its natural setting, with the perspective of the participants uninfluenced. This then positions the endeavours to seek to understand the phenomenon within the deeper cultural and contextual situations.

The philosophical basis for the interpretive research is in hermeneutics and phenomenology. Hermeneutics can be seen as a means to analyse and suggest a way of attempting to understand meaning or to explain textual (language) data that might be confusing for some or other reason (Scotland, 2012:12). The most basic principle of hermeneutics is that it focuses on the point that human understanding is achieved by following an iterative approach to the consideration of the interdependent meaning of the different parts that form a whole. Hermeneutics considers not only written text, but also everything that falls within the interpretative process such as verbal and non-verbal communication.

Phenomenology can be described as the study of phenomena. It looks at the appearance of things or the way in which things appear to us from our experiences (Scotland, 2012:12). Phenomenology is the study of structures of consciousness as experienced by a person. It attempts to create conditions for the objective study of topics typically regarded as subjective such as judgements, perceptions, and emotions. Phenomenology describes the experiences that have been lived by individuals regarding a concept or phenomenon.

Access to reality within the premise of interpretive research occurs via social constructs such as linguistics, consciousness and transferred meanings.

2.2.2.1 Ontological assumptions

Researchers who follow the interpretivist paradigm believe that reality consists of the subjective experiences people receive from the external world. They believe that interpretivism consists of multiple realities that can only be constructed through human interactions and meaningful actions

(Healy & Perry, 2000:120). It is rooted in the belief that conversations within the natural setting are the main means through which people make sense of their social worlds and that multiple social realities exist due to the differing individual experiences that encompass the views, interpretations, knowledge, and experiences they undergo (Guba & Lincoln, 1994:110).

The ontological position of interpretivism is relativism (Cohen *et al.*, 2007:11). Relativism is rooted in the view that reality is subjective and differs from person to person (Guba & Lincoln, 1994:110). It believes that our realities are shaped by our senses and that without our consciousness, the world is meaningless. There are multiple realities that are individually constructed. Language moulds reality, and therefore reality is constructed through interaction between language and aspects of an independent world (Scotland, 2012:11).

2.2.2.2 Epistemological assumptions

Interpretivism has its epistemological assumptions rooted in the view that events that occur are acknowledged through cognitive processes of explanation, which are influenced by interactions that occur within social contexts. Knowledge is socially constructed by experiencing the natural setting of the phenomenon under investigation. The researcher collects data from the research participants through an interlocked and interactive process of talking and listening. This makes interpretivism a paradigm that is more personal and interactive as a means of collecting data. The investigator and the object under investigation are assumed to be interlinked so that findings can be created as the research progresses (Guba & Lincoln, 1994:111).

The epistemology surrounding interpretivism is in that it is one of subjectivism and is based on real-world phenomena. Scotland (2012:11) goes on further to say that the world cannot exist independently of our knowledge. Interpretivism accepts ideologies and does not question them.

2.2.2.3 Methodology

The methodology applied in interpretivistic research is that data is typically collected through questionnaires and interviews. The research product is based on the values of the researcher through descriptive analysis and emphasis of a deep and interpretive understanding of the social phenomenon. The researcher will therefore need to be immersed in the research process and will therefore not be perceived as being entirely objective is his views.

The interpretive methodology seeks to understand the phenomena from an individual perspective then investigating the interaction occurring between the cultural and historic context that people inhabit (Guba & Lincoln, 1994:111). The methodologies that are encompassed within

interpretivism include phenomenology, hermeneutics, and ethnography (Scotland, 2012:12). Table 2-4 provides a brief description of these research methodologies.

Table 2-4: Some of the research methodologies employed in the interpretivist paradigm (Scotland, 2012:12)

Name	Description
Phenomenology	Seeks to study experiences without interfering with existing preconceptions.
Hermeneutics	Seeks to derive hidden meaning from language.
Ethnography	Seeks to study cultural groups over a prolonged time.

2.2.3 Critical social theory

Harvey (1990:4) describes critical social research as research that is "*underpinned by a critical-dialectical perspective which attempts to dig beneath the surface of historically specific, oppressive, social structures.*" It is knowledge that is seen by social theorists as being structured by existing sets of relations that are oppressive (Goede, 2004:17). Harvey (1990:5) goes on further to say that critical social research is structured by existing sets of social relations and that it primarily aims to provide knowledge that will engage the social structures that prevail. The critical researcher therefore sees social structures as being oppressive, which can either fall into a category of being oppressive by class, race, or gender. The paradigm of critical social theory therefore, according to Cohen *et al.* (2007:26), and as referenced by Scotland (2012:9), is a paradigm that aims to emancipate individuals and groups into an equal society. Its purpose is not to merely understand situations and phenomena, but also to change them by emancipating the disempowered and redressing inequality to promote freedom from within a democratic society.

Critical social research focuses on the basic nature of the phenomena. It takes apart the abstraction of phenomena in order to expose its deeper intricacies to reconstruct the abstract concept in relation to the socio-structural relations which form it. Critical social research regards the positivistic scientific method as insufficient in that it does not deal with what lies below the surface (Goede, 2004:27). Critical social research is therefore a paradigm that goes past surface appearances by understanding social phenomena within their particular historical context. Critical social research sees the phenomena under observation being non-specific, but related to other phenomena within a specific social structure. Critical social research examines the structure and maintains this through the exercise of political and economic power. Therefore, "c*ritical social research thus addresses and analyses both the ostensive social structure and its ideological manifestations and processes*" (Harvey, 1990:17). It directs attention at the most fundamental nature of phenomena.

2.2.3.1 Ontological assumptions

Critical social research views reality as being created and directed by social bias. It is an approach of the world that involves locating methodic concerns within an epistemological framework (Harvey, 1990:9). Harvey (1990:17) goes on further to say that critical social research concerns the revelation of the underlying social relations and expressing the structural and ideological forms.

Critical social theory is of the ontological position of historical realism. Guba and Lincoln (1994:110) as well as Scotland (2012:13) make a point that historical realism is a view of reality that has been shaped by gender values, political values, economic value, ethnicity, cultural and social values.

2.2.3.2 Epistemological assumptions

Critical social research is of the epistemological view that knowledge and critique are connected. Knowledge gets created through social constructs and is influenced by power relations within society (Scotland, 2012:13). Critical social research describes the methods or interventions that change oppressive structures to emancipate those who are oppressed. It aims to cut through surface appearances as opposed to the positivistic scientific method that only deals with the surface of social appearances (Harvey, 1990:17). Critical social research aims to analyse social processes by unpacking conceptual frames with the intention of revealing the underlying practices and their particular structural and historical manifestations. This is achieved by obtaining knowledge. This knowledge is seen as "*a process that is moving towards an understanding of the world and of the knowledge which structures our perceptions of that world*" (Harvey, 1990:3).

2.2.3.3 Methodology

Critical social theory "*adopts pluralistic inquiry methods that are heavily oriented towards interpreting and mapping the meaning and social construction of the universe of inquiry*" (Ngwenyama, 1991:355). By adopting a pluralistic inquiry to interpreting and mapping meanings of social construction of the universe inquiry, the researcher can be cognisant of the real-life experience of the participants. The analysis of the social context uses active participation, observation, and analysis of the contextual data.

There are several elements, as identified by Harvey (1990:17), used within the context of critical social research which are "*abstraction, totality, essence, praxis, ideology, history, and structure, as well as deconstruction and reconstruction*". Table 2-5 provides a brief description of these elements that are used within critical social research.

Table 2-5: Some of the research methodologies employed in critical social theory research (Harvey, 1990:17)

Name	Description
Abstraction	Accepts that fact cannot exist apart from reality and derives abstracts concepts to concrete ones.
Totality	The social phenomena is interrelated and together form a whole. The phenomena is not investigated alone but alternatively as part of a larger context.
Essence	It is the basic component of an analytical process. It seeks understanding of the interactive processes and as a fundamental concept that can be used to reveal the deconstructive process.
Praxis	A practical reflective activity that seeks to change the world. It views knowledge as not being static, but rather as a constantly changing aspect as a result of reflection and action.
Ideology	Expresses two perspectives of ideology and nature, which are the positivist view and a negative view.
History	It is the reconstruction of previous events and processes.
Structure	It is the aggregation of all other elements and is viewed in its whole as part of a complex and interrelated set of elements which are independent and equal when viewed as a whole.
Deconstruction and reconstruction	Refers to beginning from the point of abstract concepts that are applied, or are related, to an area being investigated and then separating or deconstructing these abstract concepts.

2.2.4 Design science research

The aim of design science research is to create innovative artefacts in order to solve real-world problems. Design science is a paradigm that fundamentally seeks to solve problems (Hevner *et al.*, 2004:76). It is a paradigm that is rooted in the science of engineering and the artificial (Simon, 1996:111). The design science paradigm fundamentally seeks to "*create innovations, that define the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, management, and use of information systems can be effectively and efficiently accomplished*" (Hevner *et al.*, 2004:77). Design science research is research that creates knowledge in the form of constructs, techniques, and methods, and models through the use of design, analysis, reflection, and abstraction (Vaishnavi *et al.*, 2004/2019:4). Philosophically, according to Hevner *et al.* (2004:76), design science research draws from pragmatism in the field of information systems research. Design science research is therefore rooted in a world-view of pragmatism. It is seen as its own research paradigm in this study which joins the view of Myers and Venable (2014:801) as well as Gregor and Hevner (2013:337) as discussed in the introduction of this chapter.

Design science research is knowledge that is formed of "*constructs, techniques and methods, models, well-developed theory for performing this mapping—the know-how for creating artefacts that satisfy given sets of functional requirements*" (Vaishnavi *et al.*, 2004/2019:4). It can therefore be seen as a research approach that seeks to create knowledge using abstraction, design, reflection, and analysis.

Design science research has unique metaphysical assumptions. The ontology and epistemology assumptions of design science research are not derivable from any other paradigm. The ontological and epistemological viewpoints of design science research shift as the research progresses through the design science research cycle (Vaishnavi *et al.*, 2004/2019:9).

2.2.4.1 Ontological assumptions

Design science research seeks to change the state of the world through the introduction of innovative artefacts. It is a paradigm that is constituted of multiple but contextually situated world states (Guba & Lincoln, 1994:110). It changes the state of the world through the introduction of innovative artefacts. The paradigm is rooted in the fundamental view that there is only a single underlying physical reality that constrains the multiplicity of world states (Vaishnavi *et al.*, 2004/2019:9).

2.2.4.2 Epistemological assumptions

The epistemological assumptions attached to design science research are that information is factual, and that this information can be understood through a process of development and circumscription (Guba & Lincoln, 1994:110). This relates to the notion by Vaishnavi *et al.* (2004/2019:9) of knowing through making. Furthermore, the design science researcher will develop an artefact, study the behaviour resulting from the interaction of the components, and then obtain the information derived from the descriptions of interactions of the components. This will enable the researcher to determine the predictability of the behaviour of the components to conclude whether the information is true or not. The truthfulness of this information will be based on whether the behaviour of the interaction of the components within the artefact is predictable (Vaishnavi *et al.*, 2004/2019:9).

2.2.4.3 Methodology

The design science research methodology comprises three elements, namely the conceptual principles that define what is meant by design science research, practice rules, and lastly, a process for conducting and presenting the research (Peffers *et al.*, 2007:49).

Vaishnavi *et al.* (2004/2019:22) define a DSR theory development framework, which is further extended by Peffers *et al.* (2007:50) to define the DSR process model. The activities for both these methodologies are compared in Table 2-6.

Table 2-6: A mapping of the activities in design science research methodologies as defined in the design science research process model by Vaishnavi *et al.* (2004/2019:11) and the design science research methodology process model by Peffers *et al.* (2007:52)

Design science research process model activities	Design science research methodology process model activities
1. Awareness of problem	1 Identify problem & motivate 2. Define objectives of a solution
2. Suggestion 3. Development	3. Design & development
4. Evaluation	4. Demonstration 5. Evaluation
5. Conclusion	6. Communication

2.2.5 Positioning the study in DSR

The primary objective of this study is to design and develop an artefact that can be used to raise awareness about social engineering attacks among administrative staff in medium to large organisations.

The research paradigm chosen for this particular study is design science research, specifically because the problem and purpose of the study is to solve a real-world problem through the development of an artefact. Design science research does just that, it solves real-world problems through the creation of a new and innovative artefact. The positivistic paradigm was also suitable in that it is empirical and relies on measurement to verify truth through observation; however, its objective does not require the creation of an artefact, but rather the verification of a hypothesis or theory. The qualitative data used in this study for richer context on the design of the artefact does not relate to positivism's goals. Critical social theory could be applicable; the reason for this is that the research intends to assist people in avoiding being victims to social engineering attacks. However, the primary focus of this study is on the design of the artefact and not yet on the emancipation of its users.

Interpretivism could also be an applicable paradigm in that it is subjective and obtains meaning through the observation of social interactions (hermeneutics and phenomenology). However, the

interpretive paradigm does not satisfy the requirement for artefact creation past the *understanding* of the social interactions, which indicates it is not a suitable paradigm for this research.

It is important to note that, because the goal of the study is to develop an artefact, the study is therefore positioned in the design science research paradigm to guide the design process. From the discussion of design science research in Section 2.2.4, it is indicated that design science research is rooted in the worldview of pragmatism. Pragmatism advocates the use of both qualitative and quantitative research methods, which are based on the needs of the specific study (Kivunja & Kuyini, 2017:38). It therefore draws its research methods such as questionnaires, interviews, etc. from other paradigms for evaluation. The next section will evaluate some of these research methods.

2.3 Data gathering methods

Data comes in two main forms, either as primary data or secondary data (Walliman, 2011:71). The data can further be categorised as either being quantitative or qualitative (Chu & Ke, 2017:285). This section will describe these concepts in further detail.

2.3.1 Primary and secondary data

Primary data is data that is gathered *first hand* (Rabianski, 2003:43). It is data that is obtained through observation, experience, or through recording as close to the phenomenon as possible (Walliman, 2011:69).

Secondary data, on the other hand, is data that has been interpreted and recorded (Hox & Boeije, 2005:593). This data is obtained through written sources (Walliman, 2011:70). This means that the data is not compiled by the analyst, but is rather collected from other sources such as published and unpublished research (Rabianski, 2003:43).

It is these factors that make primary data more reliable and the data that bring us closest to the truth (Hox & Boeije, 2005:594). What makes secondary data less reliable is that the facts may have been distorted by another individual's non-factual perceptions (Walliman, 2011:71).

To put these two forms of data into perspective, one could imagine primary data as data that was gathered through experience; an example would be experiencing a virus attack on your personal computer, which makes the information obtained very direct. Secondary data would come from another source such as a newspaper article illustrating the event and is therefore not from a direct experience.

2.3.1.1 Types of primary data

There are typically four types of primary data, which is distinguished primarily by the way in which it is collected. Primary data is data that can be collected through participation, observation, measurement, and interrogation (Hox & Boeije, 2005:595). Measurement would entail gathering data through numbers that indicate amounts; observation would be gathering information through senses or an instrument such as a camera; interrogation would be gathering data through asking questions; and lastly, participation, which would be data gathered through bringing people (also referred to as participants) together typically into a participatory design session, and asking them to do things (Walliman, 2011:70).

2.3.1.2 Types of secondary data

Secondary data is the type of data that has been recorded or interpreted, which may come from sources such as newspapers, bulletins, magazines, journals etc. (Hox & Boeije, 2005:593). A major aspect to consider before using secondary data is that it requires extensive review to determine its validity before it can be used in formal research (Walliman, 2011:70).

In addition to the fact that data can be divided into two types, as primary and secondary data, it can further be categorised as either quantitative or qualitative (Hox & Boeije, 2005:593).

2.3.2 Quantitative and qualitative data

Quantitative data can be measured in numbers using statistical methods, which allow it to yield some form of accuracy as compared to qualitative data (Williams, 2007:66). Qualitative data tends to be less accurate than quantitative data in that it cannot be accurately quantified using numbers, but is rather expressed in the form of words (Walliman, 2011:131).

There are a number of differences between quantitative and qualitative research. Table 2-7 lists the specific differences between quantitative and qualitative research.

Table 2-7: Comparison of quantitative and qualitative research approaches (Slevitch, 2011:79)

	Quantitative approach	**Qualitative approach**
Worldview (paradigm)	Realism/positivism.	Idealism/constructivism.
Ontology (views on reality)	Provides a single, independent and objective reality that can be known or described as it is in the true reality.	Accepts multiple social realities which are not describable independent of people's perspectives, values, interest or purposes.

	Quantitative approach	Qualitative approach
Relationship between facts and values	It is possible to separate facts from values as a results of the segregation of the world and mind.	Facts are inseperable from values because social inquire cannot be valueless.
Epistemology (views on knowledge)	Dualist/objectivist.	Subjectivist.
Methodology (aims of scientific investigation)	Experimental/manipulative.	Hermeneutical/dialectical.
Methods (research techniques and tools)	Methods includes measurements, randomisation, hypothesis testing, structured protocols, etc.	Methods include filming, focus groups, observations, case studies, interviews, etc.

Quantitative research enables the researcher to familiarise himself with the study at hand, and allows him to generate the hypotheses to be tested. Quantitative research emphasises facts, it is quantifiable in the form of numbers, and uses mathematical processes for analysis of the numbers that are expressed in the form of statistical terminologies (Golafshani, 2003:597). Qualitative research, however, is a naturalistic approach that tries to understand the phenomena within a context without the researcher manipulating the phenomena being studied (Thomson, 2011:78).

Chu and Ke (2017:292) point out that research methods will not always only result in quantitative *or* qualitative data, but can include both types.

2.3.2.1 Quantitative data analysis

Quantitative data analysis is a research method that involves the analysis of numeric and statistical input (Hox & Boeije, 2005:595). It seeks to objectively measure reality and create meaning through uncovering the objectivity in the data that is collected (Williams, 2007:66).

There are three general classifications to quantitative research, namely descriptive, experimental, and causal comparative (Williams, 2007:66). These classifications are described as follows:

(i) The descriptive approach identifies attributes of a specific phenomenon based on observations and correlation of phenomena;

(ii) Experimental research involves investigating a treatment into a study group and the outcomes thereof; and

(iii) Causal comparative research examines the effects the dependent and independent variables have on each other, as well the cause and effect between them.

In addition to the aforementioned classifications, Golafshani (2003:600) indicates that there is a fourth classification, which is surveys.

Quantitative data is typically gathered through surveys and questionnaires. The methods are well structured and developed and can provide statistical data which can be analysed through statistical means in order to provide abstraction to a larger population (Anonymous, 2014:9).

2.3.2.2 Qualitative data analysis

Qualitative research is described by Creswell (1998:14), as quoted by Williams (2007:67), as an unfolding model that occurs in a natural setting, which allows the researcher to involve and detail the participant's viewpoint and experiences of the phenomenon that is being investigated.

There are five commonly recommended methods for conducting qualitative research, which are mainly case studies, grounded theory, ethnography, content analysis, and phenomenology (Williams, 2007:68). According to Lacity and Janson (1994:142), there are three commonly used approaches to analysing text from qualitative data, with each being dependent on *"assumptions to include the role of the researcher*":

(i) Positivistic view approach includes content analysis, verbal protocol analysis, and script analysis;

(ii) Linguistic approach includes speech act analysis and discourse analysis; and

(iii) Interpretive approach includes hermeneutics, open coding, and intentional analysis.

Interpretive content analysis is a qualitative analysis technique that aims to provide a qualitative rendering of group behaviour with the objective of piecing together individuals' words, observations, and documents into "*a coherent picture expressed through the voices of the participants"* (Trauth & Jessup, 2000:54). Open coding is a qualitative analysis technique where units of data are labelled through concepts and themes which were identified in the data. These themes do not come from existing literature or theories (Hoepfl, 1997:55). Intentional analysis is one of the forms of the interpretive data analysis approaches that seeks to understand the speaker's intention. Intentional analysis is typically appropriate for situations where interview collected data needs to be analysed. The analysis of this data collected takes place in four steps (Lacity & Janson, 1994:151):

1. The researcher needs to describe the facts around the phenomenon;

2. The researcher needs to determine how the participants assign meaning to their distinct realities as well as how they view cause and effect;

3. The researcher identifies themes from text, and thereafter uses the themes to develop interpretations for a classification of phenomena; and lastly

4. The researcher then finds meaning for the text which are subjective themes extracted from the study of the phenomena.

Qualitative research is considered trustworthy (Williams, 2007:67). The researcher's findings should be truthful as they are gathered from the participants. This will allow other researchers to also reach the same conclusions when performing the same research approach within similar contexts and settings (Doody *et al.*, 2013:268). It is imperative that researchers carefully and clearly document their findings while performing the findings analysis and then having a peer review to verify the trustworthiness and consistency of those findings (Plummer-D'Amato, 2008:125).

2.3.3 Data collection techniques

Lethbridge *et al.* (2005:314) define six types of frequently used data collection techniques used by researchers to collect research data. These data collection techniques are interviews (structured, unstructured, or semi-structured), questionnaires and surveys, observations, focus groups, case studies, and documents. These six techniques described above are commonly used by researchers to gather research data. Table 2-8 provides a brief description of these data collection techniques.

Table 2-8: Description of data collection techniques (Walliman, 2011:96)

Technique	Description
Interviews	Interviews are a technique where individuals or interviewees are presented with exactly the same set of questions in the same order with the intent of collecting data for a statistical survey. The data within this context is collected by an interviewer where a form is filled in rather than through a questionnaire that is self-administered by the respondent or interviewee in this case. This approach is achieved primarily through telephonic interviews, face-to-face interviews, or computer assisted personal interviews (CAPI). Interviews can be structured, unstructured, or even semi-structured.
Questionnaire	Questionnaires are a technique where data is gathered through the presentation of a list of questions to individuals. The questions are often compiled in the form of a checklist or a ratings scale (often referred to as Likert scales). This approach is typically achieved through the use of mail questionnaires or web-based questionnaires.
Observation	Data is gathered just by observing a phenomenon and not asking questions. The researcher is generally detached from the phenomenon and does not get involved.

Technique	Description
Focus groups	These are conducted by assembling a group of people together with the aim of allowing them to discuss and reveal their opinions and beliefs about a specific subject of the research.
Case study	When the researcher needs to draw up conclusions about the entire population using a sample or subset of the group, they call this sampled subset a case study.
Documents	This is achieved by examining physical records such as papers, documents, etc. and then transforming the collected accounts into working documents that can be coded and analysed.

The sections below will provide more detail on what these techniques are and how they are employed during research.

2.3.3.1 Interviews (structured/semi-structured/unstructured)

According to Anderson (1990:222), an interview can be seen as a specialised form of communication that takes place between people for a specific purpose, associated with some agreed upon subject matter.

Interviews come in three categories, which are structured, semi-structured, and unstructured. Structured interviews are when a researcher comes with a prepared list of questions for the interview. Unstructured interviews are when the researcher does not bring a prepared list of questions to the interview. When the researcher asks only a part of the prepared interview questions, but also asks follow-up questions that are not prepared for, then it is a semi-structured interview (Chu & Ke, 2017:289).

When conducting interviews, there are some subtle surrounding factors that the researcher needs to keep in mind in order for the interview process to run smoothly. The researcher needs to ensure that a suitable location is selected to conduct interviews, typically a place that is free from interference. It is also imperative that the number of questions to be asked be kept in consideration, including both the content and process functions thereof (Dilshad & Latif, 2013:194).

2.3.3.2 Questionnaires

Questionnaires, or sometimes known as surveys, can be used to gather both quantitative and qualitative data (Walliman, 2011:97). Using this form of data collection technique allows the researcher to obtain data without having to ask a particular set of questions to the respondents. From the studies by Jerry Chih-Yuan *et al.* (2017:48) and Biswas *et al.* (2019:93) it is evident that

questionnaires can be used for pre- and post-tests. The researcher will obtain the required data through the use of a list of predefined questions (Chu & Ke, 2017:290). This form of data collection technique allows the researcher to gather large amounts of data from a large group of respondents or for the purpose of multiple cases (Rabianski, 2003:45).

There are two types of questionnaires, which can be either open-ended format questions, or closed-ended format questions (Chu & Ke, 2017:290). Closed format questions require the respondent to choose from a set of given answers. The answers are generally quick and easy to get through; however, they limit the range of possible answers the respondent can choose from. Open format questions, on the other hand, allow the respondent to freely answer in their own content or style, which, in turn, provides them with the freedom to respond freely with a lack of bias. Interpreting and responding to open format questionnaires, however, is much more demanding for both the researcher and respondent. Questionnaires can be delivered to respondents through three main platforms, either personally, through the Internet or through post (Walliman, 2011:97).

2.3.3.3 Focus groups

Sim (1998:346) defines a focus group as a group interview that is centred on a specific topic or focus and is facilitated or coordinated by a moderator or facilitator. Focus groups seek primarily to generate qualitative data by utilising the interaction that takes place within a group setting, through the process of discussion and interactions between the group members (Chu & Ke, 2017:289). Focus groups are a technique that was commonly used since the 1920s as a method of market research. They are used as means of conducting group discussions that are organised to explore a specific set of issues from the views and experiences of different individuals (Kitzinger, 1994:103). Focus groups can be viewed as a tool in participatory research (Morgan, 1996:133).

There are several guidelines that Dilshad and Latif (2013:194) provide for constructing the questions for focus groups; these guidelines are:

(a) the focus group questions should be open ended;

(b) the questions must be of a qualitative nature;

(c) avoid questions that possibly provide yes/no answers; and

(d) use of directive approach should be avoided to know the reasons behind a particular standpoint or reaction of the participant.

As stated by Doody *et al.* (2013:266), the most suitable qualitative data analysis techniques for focus groups include constant comparison analysis, classical content analysis, keywords-in-context, and disclosure analysis. However, Plummer-D'Amato (2008:124) defines several strategies to enhance the trustworthiness of focus group data in qualitative research.

2.3.3.4 Observations

In this method, the researcher does not get involved with the subjects or phenomena, but rather observes from a distance (Chu & Ke, 2017:290). It is a technique that forms the backbone for testing scientific theories, support new discoveries, as well as improve our understanding of the natural world (Kostewicz *et al.*, 2016:19).

Researchers typically use this method to record data about events and activities, or even the nature or conditions of objects such as buildings or artefacts. These observations can range from merely a visual survey to a detailed survey that utilises a range of instruments for measurement (Chu & Ke, 2017:290).

Observation is a data collection technique used in many branches of research, specifically in the branches of the natural and technical sciences (Rabianski, 2003:44). The data collection method, however, is not only limited to these branches, but may also be used in branches such as that of the social sciences to, for example, study the behaviour of people and their activities. This method can be used to gather both qualitative and quantitative data (Walliman, 2011:97).

2.3.3.5 Case studies

A case study is a research data gathering technique that explores in great depth an event, process, or one or more individuals (Creswell, 2014:14). The structure of a case study is composed of the problem, context, issues, and lessons learned (Creswell, 1998:87). Case studies fall under a method known as sampling. Sampling is used when a researcher wishes to obtain information about a large group of items that would otherwise take the researcher too long or would be restrictive due to other resource constraints. The researcher would then only examine a subset of the entire population in the hope that the subset that was collected would be representative of the entire population. This collected subset would represent typical features to that of the entire population (Walliman, 2011:93). Case studies are typically well suited for research that aims to explain or describe a particular phenomenon and develop a hypothesis or theory (Kjeldskov & Graham, 2003:319).

Data collected for a case study can stem from multiple sources, which can include observations, interviews, documents, physical artefacts, or even audio-visual material (Williams, 2007:68). It is

important that the researcher understands that sometimes these case studies show differing characteristics. Sometimes, the researcher may want to examine the dynamics of different groups and not isolated items. To accomplish this, the researcher will select several items from the groups that show extreme characteristics of the phenomenon under observation to create a new sample group; he will then evaluate these new sample groups and subsequently draw conclusions on them (Walliman, 2011:91).

2.3.3.6 Documents

Documents can be described as any information that is either public such as newspapers, meeting minutes, official reports, etc., or information that is private such private journals, letters, e-mails, etc. (Creswell, 2014:190).

The authenticity of the accounts recorded from the participants needs to be cross-checked with other people's accounts who were involved through the examination of physical records of events such as reports, papers, documents, etc. The accounts collected from the respondents will need to be transformed into working documents that can be coded and analysed (Walliman, 2011:95). The analysis of the documents will be a systematic procedure of reviews and evaluations that can provide background and context, additional questions to ask, supplementary data, as well as being a source for verifying findings (Bowen, 2009:30).

The different research approaches that can be employed within the four research paradigms were discussed in Section 2.3. Design science research as the chosen paradigm of this study is expanded on in Section 2.4 through a discussion of its frameworks, guidelines, methods, and ethics thereof.

2.4 Design science research

Design science research can be described as a group of analytical techniques and views that are used to perform research within the information systems field. It seeks primarily to improve and understand the behaviour and specific aspects of information systems through the process of generating new knowledge by creating unique artefacts, as well as by analysing their use and performance (Vaishnavi *et al.*, 2004/2019:1). Hevner and Chatterjee (2010b:5) support this definition by stating that design science research is a research paradigm that creates new knowledge through a process of designing innovative artefacts.

Information systems are known to be complicated, unnatural, and designed for a purpose within the setting they represent. The information systems are made of people, technologies, structures, as well as work systems. Figure 2-1 illustrates the essential alignment between business and

information technology strategies and also the alignment between the organisational and information systems infrastructures (Hevner *et al.*, 2004:78).

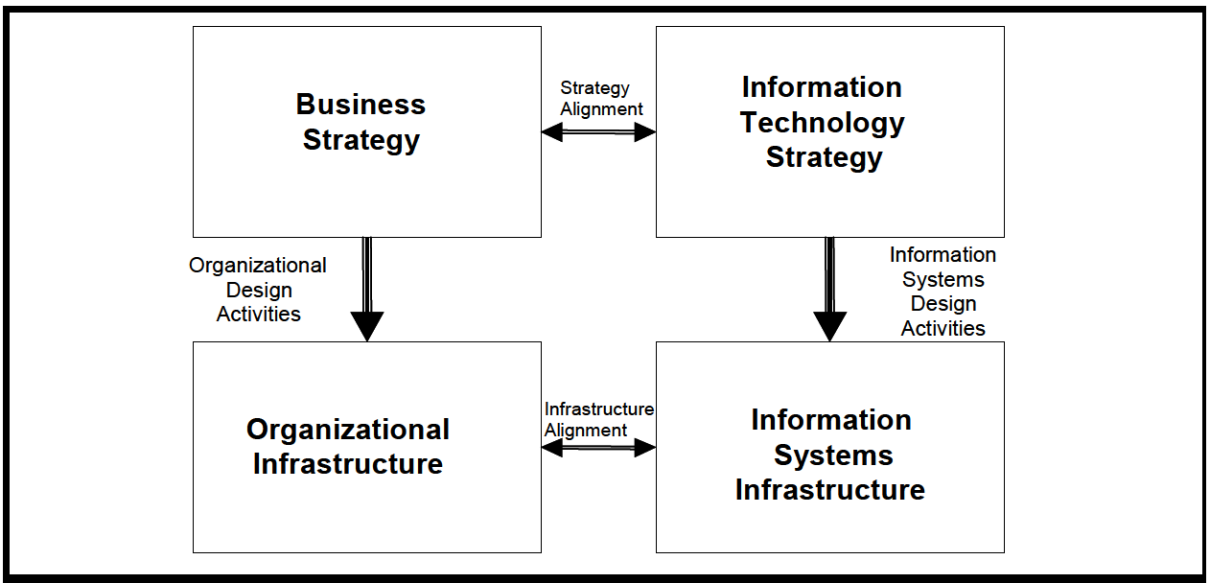


Figure 2-1: The organisational design and information systems design activities (Hevner *et al.*, 2004:79)

To construct information systems (IS) that are used to solve complex and sometimes simple business problems, some type of methodology is needed to be followed in order to maximise the impact these designs bring to organisations through rigorous evaluation and knowledge generation. Design science research is an IS research paradigm which involves the process of constructing a variety of "*socio-technical artefacts using behavioural and design science paradigms*", such as a new software, process, algorithm, or system that is purposefully designed to solve or enhance an identified problem (Myers & Venable, 2014:801). In summary, design science research (DSR) is "*the research methodology used for the creation and evaluation of an artefact for information systems*" (Gregor & Hevner, 2013:337). A design science study represents four general aspects (Baskerville *et al.*, 2015:543):

1. A design-science research project;
2. The development and design (evaluating and building) of an artefact which is based on the research study;
3. The development and design process producing new knowledge; and
4. The DSR project being described by the creation of reports or articles.

Section 2.4.1 describes the DSR frameworks as defined by Vaishnavi *et al.* (2004/2019:23) (the DSR process model), Peffers *et al.* (2007:52) (the DSRM process model), and Hevner (2007:2) (the DSR cycles) in further detail. Section 2.4.2 describes the evaluation methods for evaluating the utility, efficacy, and quality of an artefact. Section 2.4.3 describes the design science research guidelines for performing design science research and Section 2.4.4 describes the possible approaches for reporting on design science research. Section 2.4.5 describes the ethical considerations for performing design science research.

2.4.1 Research frameworks for DSR

In a study by Kuechler and Vaishnavi (2012:396), they specify a framework for theory development that follows three general activities, which are as follows:

1. The development of an artefact which is guided by practice-based insight or theory;
2. An evaluation of the artefact through a process of gathering functional performance data which is based on the artefact's performance; and
3. Reflecting on the outcomes gathered from the process of the design of the artefact and the implications thereof on the artefact.

In the next section, three models for performing design science research are discussed. The three models are (1) the DSR process model, (2) the DSRM process model, and (3) the DSR cycles.

2.4.1.1 Design science research process model (from Vaishnavi *et al.* (2004/2019:8))

The design science research process model developed by Vaishnavi *et al.* (2004/2019:8) is an extension of the computable design process model developed by Takeda *et al.* (1990:40). A design science research effort typically follows five steps, which are: (1) awareness of a research problem, (2) suggestion of a problem solution, (3) development of the artefact, (4) evaluation of the artefact, and (5) conclusion on the research efforts. Figure 2-2 provides a summary of these five steps, with a depiction of the knowledge flows and outputs for each of the process steps.

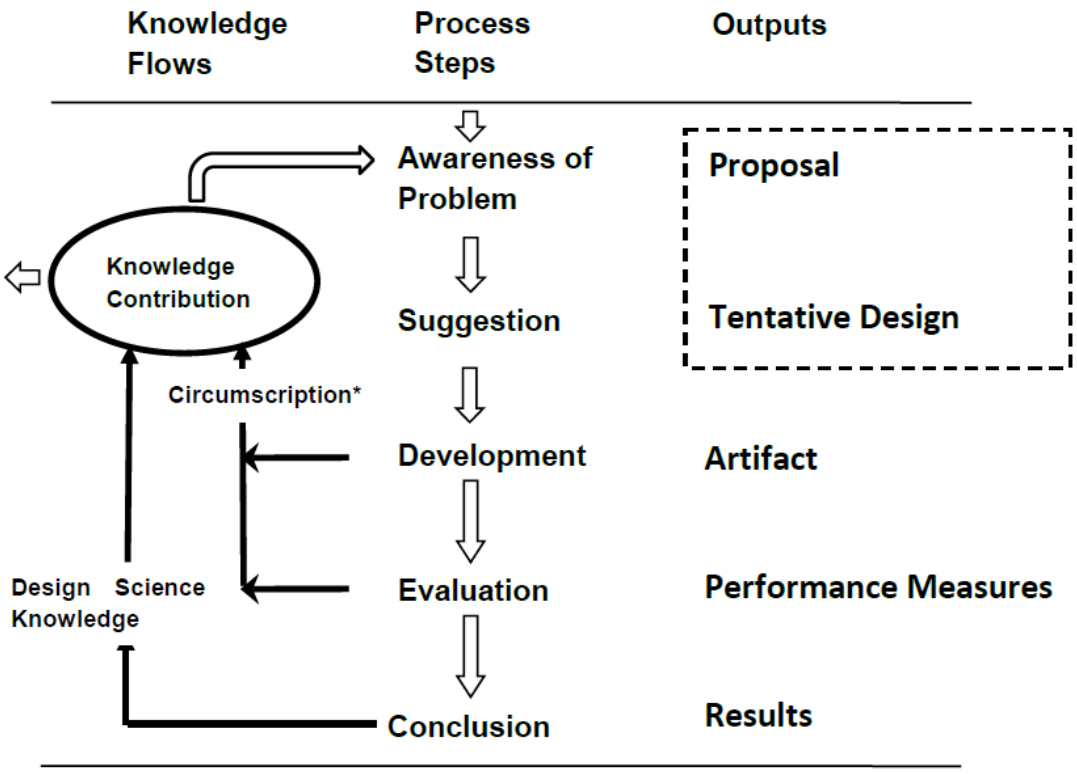


Figure 2-2: The design science research process model (Vaishnavi *et al.*, 2004/2019:8)

The process model steps are described.

Awareness of problem

This step of the research process is the identification or awareness of a research problem with the output of a proposal for endeavouring the research problem. The problem identification can be sparked by input from multiple sources, or simply from a new development in the industry. DSR efforts are typically problem-solving oriented as opposed to question-answer.

Suggestion

Suggestion follows the proposal, and the output thereof is a tentative design that is based on the proposal. "*Suggestion is essentially a creative step wherein new functionality is envisioned based on a novel configuration of either existing or new and existing elements*" (Vaishnavi *et al*., 2004/2019:9). The process of envisioning should yield a tentative design, which if it does not, it will be set aside.

Development

From the suggestion step, the tentative design is further developed and implemented. The output of this step is an artefact that can be implemented in various ways depending on the specific design. Artefacts can range from design theories, instantiations, processes, models, to concepts.

Evaluation

The artefact from the *development* step is evaluated against the criteria defined in the *awareness of problem* step. Any deviations that occur during the evaluation are noted. Two focuses on artefact evaluation are noted, one being the utility of the artefact and the other being the artefact fitness within an environment.

Conclusion

This step would typically either mark the conclusion of a research cycle or the conclusion of a particular research effort. The results of the research effort are consolidated and written up. "*Knowledge gained from the effort are categorised as firm (facts learned that are repeatable in their application) or as loose end (anomalous events that need further research*)" Vaishnavi *et al.* (2004/2019:13). This step is very crucial in that it positions the research that is reported on and consequently sets the argument for the contribution to the research body of knowledge.

It is important to note that knowledge contribution typically occurs between the *development* and *conclusion* steps, and the knowledge being contributed between the *development* and *evaluation* happens through circumscription. Circumscription, as defined by Vaishnavi *et al.* (2004/2019:8) and extracted from McCarthy (1980:2), is the "*discovering of constraint knowledge about theories gained through detection and analysis of contradictions when things do not work according to theory*". The *conclusion* step will directly contribute to the research body of knowledge, which can either be firm or be that of loose end in nature.

2.4.1.2 Design science research methodology process model (from Peffers *et al.* (2007:54))

Figure 2-3 below provides an overview of the design science research methodology (DSRM) process model as specified by Peffers *et al.* (2007:54). It incorporates the principles, practices, and procedures that are required to perform a DSR study. The DSRM process model is composed of six activities which occur in a numeric sequence, but are not required to be followed in the numeric sequence that they appear. The type of research being performed will determine the research point of entry into the DSRM process model – which can be at any one of four research points of entry.

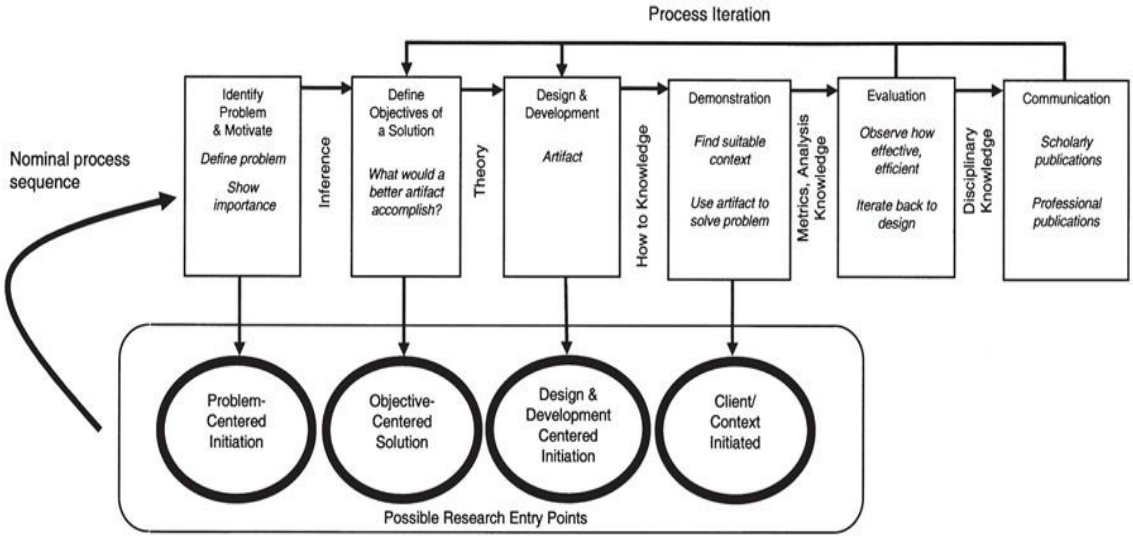


Figure 2-3: Design science research methodology (DSRM) process model (Peffers *et al.*, 2007:54)

A *problem-centred* approach will commence at the first activity and proceed further on, typically for research that resulted from observation of a problem or research from a previous project; an *objective-centred solution* would most likely be initiated by an industrial or research need and therefore, would start at activity two. Additionally, a *design and development-centred* approach may typically be started with the third activity, which typically may be as a result of an artefact that has not yet been formally thought through as being a solution that was specifically designed for the problem domain in which it will be used. Lastly, a *context-initiated* solution (activity four) may be triggered as a result of a practical solution that worked based on observation.

The synthesis of these six activities in the DSRM process model was conceived in a prior study by Peffers *et al.* (2006:91), in which work by seven authors was used to determine common process elements. Table 2-9 presents these process elements and how they relate to the synthesis of the six DSRM process model activities.

The six activities as specified by Peffers *et al.* (2007:55) that are generally followed throughout the DSRM process model are explained in further detail.

Table 2-9: Design and design science process elements from IS, other disciplines and synthesis objectives for a design science research process in IS (Peffers *et al.*, 2006:91)

Objectives for a design science research process model	Archer, 1984	Takeda *et al*., 1990	Eekels and	Nunamaker *et al.,* 1991	Walls *et al*., 1992	(Rossi *et al*., 2003	Hevner *et al*., 2004
1 Problem identification and motivation	Programming Data collection	Problem enumeration	Analysis	Construct a conceptual framework	Meta-requirements Kernel theories	Identify a need	Important and relevant problems
2. Objectives of a solution			Requirements				Implicit in relevance
3. Design and development	Analysis Synthesis Development	Suggestion Development	Synthesis, Tentative design proposals	Develop a system architecture Analyse and design the system. Build the system	Design method Meta-design	Build	Iterative search Process artefact
4. Demonstration			Simulation, Conditional prediction	Experiment, observe, and evaluate the system			
5. Evaluation		Confirmatory evaluation	Evaluation, Decision, Definite design		Testable design process/ product hypotheses	Evaluate	Evaluate
6.Communication	Communication						Communication

Activity 1: Problem identification and motivation

The first step in the design science research process requires that the researcher identify the problem and provide a reasonable justification for the value brought by the potential solution. The definition of the problem is used to develop a solution that will be in the form of an artefact and therefore requires that the problem be isolated so as to allow the solution to capture its complexity. Providing motivation for creating the solution allow for two things: (1) "*it motivates the audience and the researcher to pursue and understand the solution and accept the results*" (Peffers *et al.*, 2012:302), and (2) supports in providing a shared understating for the reasoning that is coupled with the researcher and the problem.

Activity 2: Define the objectives for a solution

The solution objectives are inferred from the problem definition as well as the knowledge of what can be done and what is technically feasible. These objectives can either be of a qualitative nature or quantitative nature. It is the researchers responsibility to infer the problem specification through rationalisation. The knowledge required to achieve the process of defining the objectives involves knowledge around the status of the problem and the solutions which are available at the time – should there be any.

Activity 3: Design and development

This activity focuses on the process of creating the artefact. These artefacts are potentially "*constructs, models, methods, or instantiations*", Hevner *et al.* (2004:78), as referenced by Peffers *et al.* (2006:90). Design science research primarily involves the design and development of an artefact with the research being embedded in the process of designing the artefact. The activity is focused primarily on specifying the artefact's intended architecture and functionality, and then ultimately in creating the artefact.

Activity 4: Demonstration

The demonstration activity typically involves demonstrating how the artefact will solve some instance(s) of a problem. This process can be achieved through a variety of platforms, including experimentation, proof, case study, simulation, as well as other activities that may be deemed appropriate for the setting. The resources required for this activity would include the effective knowledge on how the artefact is to be used to solve the identified problem.

Activity 5: Evaluation

The evaluation activity typically involves a process of observation and measurement of the artefact's performance in solving the problem observing and measuring how well the artefact provides a solution to the problem. Objectives of the solution would be compared to the actual observed results during the artefact demonstration. Knowledge around the metrics and analysis techniques would be required to accomplish the objective of this activity. Evaluation of the artefact could take many forms; the forms would be dependent on the nature of the problem that the artefact seeks to address which could ultimately include quantitative and qualitative measures. The research can iterate back to activity three (3) (design and development) or can continue on to activity six (6) (communication), which would leave the artefact open for future enhancement in future research projects. The nature of the research will determine whether such further iterations would be feasible or not.

Activity 6: Communication

The research problem as well as its relevance are communicated, including the artefact's design rigor, its usefulness and uniqueness, the foundation of its design, as well as its effectiveness toward researchers and other practising professionals.

The activities embedded in the design science research process model are ordered in sequence, but do not exhibit the explicit requirement that the process be followed sequentially. The researcher may commence from any activity and navigate outbound through the process. The research may be from either a problem focused approach, an objective focused approach, a design and development focused approach, or a context-initiated approach.

2.4.1.3 Design science research cycles (from Hevner (2007:2))

Hevner (2007:2) encapsulates the design science research process into three cycles, namely the relevance, rigor, and design cycles. The relevance cycle of the design science research process bridges the design science activities with the context of the research project. The rigor cycle brings together the DSR activities with the knowledge from scientific foundations, expertise, and experience that inform the research project. The central design cycle iterates between the activities of both building and designing artefacts and research processes (Hevner, 2007:2). Figure 2-4 depicts the three inherent DSR cycles.

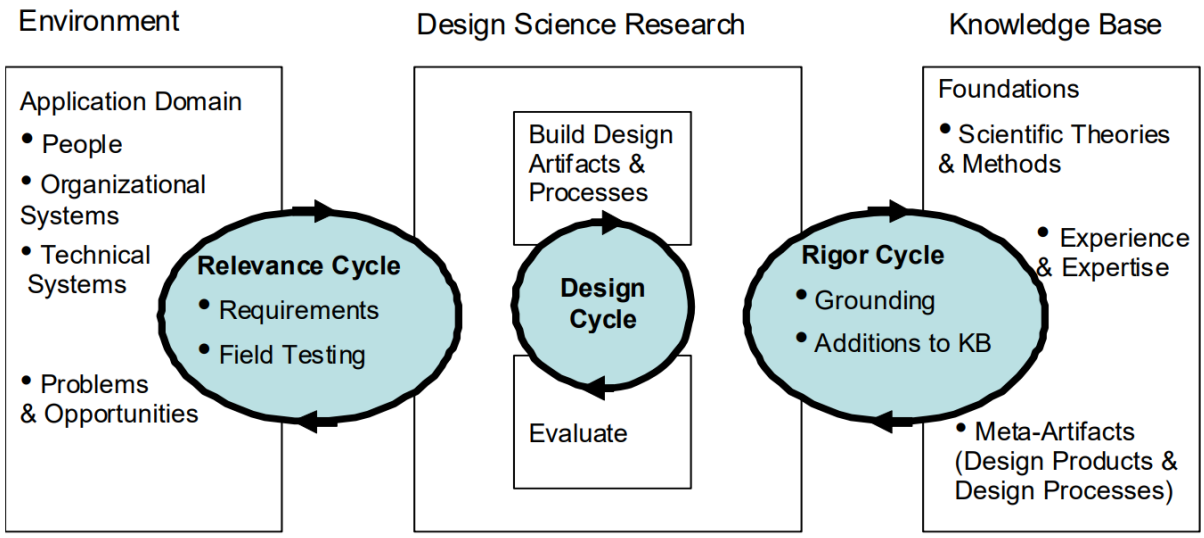


Figure 2-4: The design science research cycles (Hevner, 2007:2)

The relevance cycle

The relevance cycle initiates the DSR process and seeks to provide the requirements of the research through the identification of an opportunity or problem that needs to be addressed. An application context accepts inputs and provides a definition of the acceptance criteria for evaluating the end results. Within this cycle lies the application domain, which consists of "*people, organisational systems, and technical systems*" that are working together toward accomplishing a specific goal (Hevner, 2007:3). The question that typically arises during a design science research study is whether the designed artefact will enhance the information systems environment, and whether the improvement is measurable. Field testing will determine whether the artefact requires any additional iterations within the relevance cycle over the course of the study; this will determine whether the artefact has any deficiencies in its functionality or inherent capabilities and qualities. Additionally, field testing may also be used to determine whether the input to the design science research was adequately defined and whether the designed artefact was adequate in satisfying the problem presented. Any additional iteration to the relevance cycle will commence with input from the environment's field testing, which will ultimately redefine the actual requirements that were discovered from the field experience (Hevner, 2007:3).

The rigor cycle

Design science has its foundations rooted in the research body of knowledge from the methods of engineering and scientific theories which provide the basis for a robust DSR study. This body of knowledge contains two types of knowledge:

1. Experience and expertise defining the application domain of the research; and

2. The existence of artefacts and processes that are contained within the application domain.

The rigor cycle seeks to bring innovation to the research project through previous knowledge. It is important that researchers rigorously study and reference the aforementioned body of knowledge so as to be able to create a new and innovative design rather than routine designs that are based upon well-known processes. Research rigor in DSR is based upon the researcher's skilled ability in selecting and applying the relevant theories and methods in building and ultimately evaluating the artefact. Additions to the knowledge base will include additions made to prior theories and methods as well the additions that are as a result of field testing the artefact within its environment (Hevner, 2007:4).

The design cycle

The internal design cycle sits at the centre of any design science research project. In order to refine the design of the artefact, the design process iterates concurrently between the artefact's construction, evaluation, and subsequent feedback. The nature of the design cycle seeks to produce design replacements in relation to some defined requirements until a design that is sufficient is reached (Simon, 1996:121). The requirements are in the form of inputs from the relevance cycle, while the design and evaluation theories and methods are extracted from the rigor cycle. Hevner (2007:5) suggests that a balance should be maintained between the efforts spent on constructing and evaluating the artefact's design. As a result, multiple iterations of the design cycle should be performed before any meaningful contributions are released into the rigor and relevance cycle.

2.4.1.4 Preferred approach for this study

For this particular study, the design science research methodology (DSRM) process model by Peffers *et al.* (2007:54) is used to guide the research document. It guides the structure of the DSR research. The research objectives to this study are refined by structuring them according to the six activities of the DSRM process model as described in Section 2.5.1.1. The six activities were described in Section 2.4.1.2.

The design science research cycles by Hevner (2007:2) are described in Section 2.4.1.3. The design science research cycles are used to guide the process of designing, developing, and evaluating the artefact. The artefact will be created through a cyclical approach until a final product is reached. The design will be based on a list of requirements gathered from different sources until a conceptual design is developed. The conceptual design will be continually improved until a usable artefact has been created. This cyclical approach is favourable in that it involves the target users extensively throughout the design and development process, which ensures that the artefact adequately meets the target user needs. Throughout the design process, novel knowledge will be contributed to the research body of knowledge by obtaining inputs, evaluating them, and then recording them as novel knowledge or as contributions to the existing research body of knowledge. The process of designing an artefact, evaluating the artefact, and finally reporting on the findings that stem from the evaluation of the artefact aligns well with the four general aspects that make for a design science research project, as described by Baskerville *et al.* (2015:543).

2.4.2 Design evaluation

Design evaluation forms a critical part of the research process in that the utility, efficacy, and quality of the artefact are rigorously tested through exceptionally performed evaluation methods (Hevner *et al.*, 2004:85). The performance of the artefact can be evaluated using metrics. DSR researchers need to assess the appropriateness of their metrics, which forms an important part of the design-science research process (Hevner *et al.*, 2004:88).

Measurement of the product's quality is a factor that will take precedence in this study as the focus lies on the design of the artefact. The prototyping process is broken down into three significant characteristics, namely: (a) extensive usage, (b) iteration and formative evaluation, and also, (c) user involvement. According to Van den Akker *et al.* (2012:125), a prototyping process is critical when aiming to design a quality artefact. Van den Akker *et al.* (2012:126) define a framework that may be used to evaluate the concept of quality, which is divided into three criteria, namely: (1) validity, (2) practicality, and (3) effectiveness. An artefact's quality is firstly determined by the material that is being used to create it. The material should have content validity, in that the components of the material should be based on what is best available for use; the material should also contain construct validity in that all the components should be linked to each other. Secondly, the artefact should be easy to use and reach its ultimate goal by satisfying the user's needs as was intended by the designer. In order for the artefact to be deemed practical, there should exist consistency between both the intended, perceived, and operational curriculum. Thirdly, for the artefact to be deemed effective, it needs to satisfy and fulfil the need of the user by reaching the desired objective.

The requirements on which the artefact will be evaluated are based on the business environment for which it is designed. The environment is composed of the technical infrastructure that has been established incrementally through the implementation of novel artefacts. Evaluation of the artefact requires the appropriate definition of metrics and possibly the gathering and analysis of the data. The evaluation of the artefact can be performed on the basis of criteria such as the usability, performance, consistency, completeness, functionality, as well as any other quality attributes that may be considered relevant (Hevner *et al.*, 2004:85).

The design process is iterative and incremental in nature. The artefact design is evaluated through an evaluation process. The artefact's quality is scrutinised throughout the design and development process. The scrutiny process yields crucial feedback that is used to enhance the artefact's construction. The artefact design is only considered final and effective once it is able to adequately satisfy the purpose for which it was designed. DSR project often commence with simplistic representations and conceptualisations of problems.

The methodologies typically used for the evaluation of the designed artefact are summarised in Table 2-10 below. It is important that the selection of the evaluation methods appropriately align with the designed artefact.

Table 2-10: Summary of the design evaluation methods (Hevner *et al.*, 2004:86)

Evaluation category	Methods
1. Observe	**Case study:** It is the in-depth study of an artefact within a business environment
	Static analysis: The examination of an artefact's structure for static qualities such as complexity
2. Analyse	**Architecture analysis:** The study of an artefact's fit with an information system's technical architecture
	Optimisation: The demonstration of an artefact inherent optimal properties or the optimal bounds in its behaviour.
	Dynamic analysis: Studying an artefact operation for its dynamic qualities such as performance
3. Experiment	**Controlled experiment:** The study of an artefact's qualities within a controlled environment for qualities such as usability
	Simulation: Running the artefact with simulated data
4. Test	**Functional (black box) testing:** Running an artefact with the intent of discovering failures and potential malfunctions
	Structural (white box) testing: Running an artefact with the intent to measure its metric performance
5. Describe	**Informed argument:** The justification of an artefact's utility through arguments based on the research body of knowledge
	Scenarios: Creating a scenario in order to demonstrate the artefact's utility

Another method often used in design science research is participatory design. Participatory design is a design approach that involves the non-designer throughout the various co-design activities during the design phases of an artefact. The non-designers are typically an artefact's external stakeholder or any potential user (Sanders *et al.*, 2010:195). The pragmatic proposition of participatory design is in that involving the users' input throughout the artefact design may potentially enhance the possibility of a successful design product (Carroll & Rosson, 2007:243). Based on similar studies by Anthony *et al.* (2012) titled '*A participatory design workshop on accessible apps and games with students with learning differences*' and Khaled and Vasalou (2014:95) titled '*Bridging serious games and participatory design'*, it is clear that the ideal number of participants that can form part of a participatory design workshop ranges between three and twelve participants. It is important to note however that the aforementioned range of participants does not apply to all participatory design workshops but is a range that can adequately cater for a study such as this. In the former study, three participatory design workshops were held in a

single day to capture artefact design requirements and was composed of four participants in each of the three workshops (12 participants in total). In the latter study, the participatory design workshops were also used to gather design requirements over three sessions, where three participants were involved in two of the sessions and ten in another. This study differs from the two aforementioned ones in that it is only targeted at participants working in medium to large organisations and that the participants are involved in the end-to-end process of designing, developing, as well as evaluating the working prototype artefact.

Spinuzzi (2005:163) defines participatory design as research or sometimes a design approach that is characterised by human involvement. It focuses on the design that aims to yield inferred or practical knowledge, systems, and useful artefacts. Participatory design draws from a variety of research methods, some of which include artefact analysis, protocol analysis, observations, and even interviews, which are all generally iteratively used in the artefact design process. These methods were discussed in Section 2.3.2.

There are a variety of ways in which learning artefacts can be evaluated, one of which is to use the four-level evaluation model by Petri and von Wangenheim (2016:995). After an artefact has been developed, a number of key criteria can be identified, which can be used to test and monitor the impact of the design on the user. An example of this is given by the four-level model (Table 2-11).

Table 2-11: Four-level model to evaluate educational artefacts (Petri & von Wangenheim, 2016:995)

Evaluation	Evaluation description and characteristics	Examples of evaluation methods and instruments
Reaction	Evaluating how participates feel about the learning experience brought about by the artefact	Questionnaires, verbal responses, as well as feedback forms
Learning	Evaluates whether the participant's knowledge or skills have improved	Pre- and post-test reviews before and after the training, observations, as well as interviews
Behaviour	Evaluates the extent of change in actions (behaviour) brought about by the learning experience over a long term	Interviews as well as observations which are conducted over a long term
Results	Evaluates how the participants impact the business environment after being introduced to the artefact	Interviews as well as observations on participants, managers, etc. and are conducted and measured over a long term

2.4.3 Design science research guidelines

According to Hevner and Chatterjee (2010a:10), knowledge creation of design science research involves two complementary but distinct paradigms. The paradigms are namely natural, or otherwise known as behavioural science, and design science (March & Smith, 1995:253). Behavioural science "*seeks to justify theories that explain or predict organisational and human phenomena surrounding the analysis, design, implementation and use of information systems*" (Hevner & Chatterjee, 2010a:10). If the information systems are to reach their intended purpose, which are to enhance the effectiveness and efficiency of an organisation, then the theories need to inform practitioners and researchers about the interactions between the technology, people and organisational components. The "*design science paradigm has its roots in engineering and the sciences of the artificial*" (Simon, 1996:5). The paradigm of design science ultimately "*seeks to solve problems by creating innovations that define ideas, practices, technical capabilities, and products through which the analysis, design, implementation, and use of information systems can be effectively and efficiently accomplished*".

There are guidelines and principles which have been developed within the DSR space for performing and evaluating acceptable DSR principles. These guidelines are described in Table 2-12.

Table 2-12: Design science research guidelines (Hevner *et al.*, 2004:83)

Guideline	Description
Guideline 1: Design as an artefact	A usable artefact must be produced that can either be in the form a method, model, construct, or instantiation
Guideline 2: Problem relevance	DSR seeks to develop solutions which are technology-based and can be used to solve imperative and relevant business problems
Guideline 3: Design evaluation	The evaluation methods used to determine the quality, effectiveness and usability of an artefact need to be thoroughly demonstrated through rigorously performed evaluation methods
Guideline 4: Research contributions	The utility of DSR can be achieved through verifiable contributions to the areas of artefact design, artefact design methodologies, as well as artefact design fundamental principles
Guideline 5: Research rigor	The DSR rigor for developing the artefact places reliance on previously established construction and evaluation methods from the research body of knowledge
Guideline 6: Design as a search process	The objective of creating an effective artefact demands the utilisation of what is currently available as a platform for reaching the intended outcomes while complying with the laws prevalent within the problem environment
Guideline 7: Communication of research	The presentation of a DSR must cater for technical and management oriented audiences

The next section will discuss some of the methods for reporting on a design science research project.

2.4.4 Reporting on DSR

A study performed by Mckenney and van den Akker (2005) details the principles of how they carefully documented the iterative process of analysing, prototype designing, evaluating, and revising a computer-based program known as the '*Computer Assisted Curriculum Analysis, Design and Evaluation for Science (and mathematics) Education in Africa (CASCADE-SEA)*'. The principles that will be specified are key to the reporting approach that will be employed in this study. The detail surrounding the artefact itself will not be discussed, but rather the processes employed to evaluate and report on it.

The artefact was evaluated (for quality) in terms of three criteria, namely: (1) ***validity***, (2) ***practicality***, and (3) ***impact potential*** (Mckenney & van den Akker, 2005:47). ***Validity*** refers to the "*state-of-the-art knowledge offered in an internally consistent fashion*". ***Practicality*** refers to the way the tool caters for and contributes to the target setting. The ***impact potential*** looks at the possible change that the successful yielding of better quality materials could provide.

Additionally, three phases were employed in the evaluation of the artefact, which were a "*(a)* ***needs-context analysis****, (b)* ***design-formative evaluation*** *of prototype tools, and (c)* ***summative assessment*** *of the final product*". The main analysis phase had sought to provide an enhanced understanding of the ***needs and context*** of the artefact through a study of the literature and visiting the environment where the artefact was utilised. The second phase involved the ***design, development*** as well as the ***formative evaluation*** of four prototypes, which explored the potential impact of the artefact when used within its context. Lastly, an explorative ***query*** was conducted of other contexts and situations in which the artefact or revised version would have been useful. The sets of quality aspects identified in the Mckenney and van den Akker (2005:48) are depicted in Table 2-13.

Table 2-13: Quality aspects for designing, developing and evaluating the CASCADE-SEA program (Mckenney & van den Akker, 2005:48)

	Traits / Quality	Content	Support	Interface
Validity	State-of-the-art knowledge	Curriculum design and development knowledge; Related professional development knowledge	Advice on materials design; Guidance on embedding materials in professional development	Maximise the potential of modern ICT facilities

	Traits / Quality	Content	Support	Interface
	Internally consistent	Ideas in various components are in line with those in other areas	Tips guidelines, templates, advice and help functions are perpetually offered in a consistent fashion	Functions as intended, regularly
Practicality	Instrumentality	Guides the user step-by-step in making materials; offers freedom to work at own pace and in own style	Explains how to use program clearly and concisely	Buttons, navigation, and functions are clear
	Congruence	Links up with the needs, wishes and context of the users	Support is relevant and usable	Interface feels nice and safe, users are not alienated but motivated to use the program; Operates on technology that is available in the target setting
	Cost	Content should include enough of what users need, and not hog them down with unnecessary steps	Support should be extensive, lowering the threshold of investment cost of the user	Interface should reflect the flexibility of the system, in which users determine how they would like to go through the program (maximum degree of freedom, minimum allowance for error)
Impact potential	Yields better quality materials	The materials that are developed through the use of the CASCADE-SEA should be valid, practical, and effective	The materials that are created with the CASCADE-SEA should contain clear, useful procedural specifications	The materials that are generated with the CASCADE-SEA should evidence attention given to form and style
	Enhances the professional development of users	CASCADE-SEA should help users to think about the materials development in a (more) systematic and thorough fashion	Teaches users where resources can be found (inside the program), and how they may be used and/or adapt for own setting	Interface helps (teams of) user to visualise the process of materials development and make their work more transparent

Figure 2-5 depicts the three phases which include eight cycles that occurred over the three phases. The number of participants involved as well the duration of each cycle are also depicted within the figure.

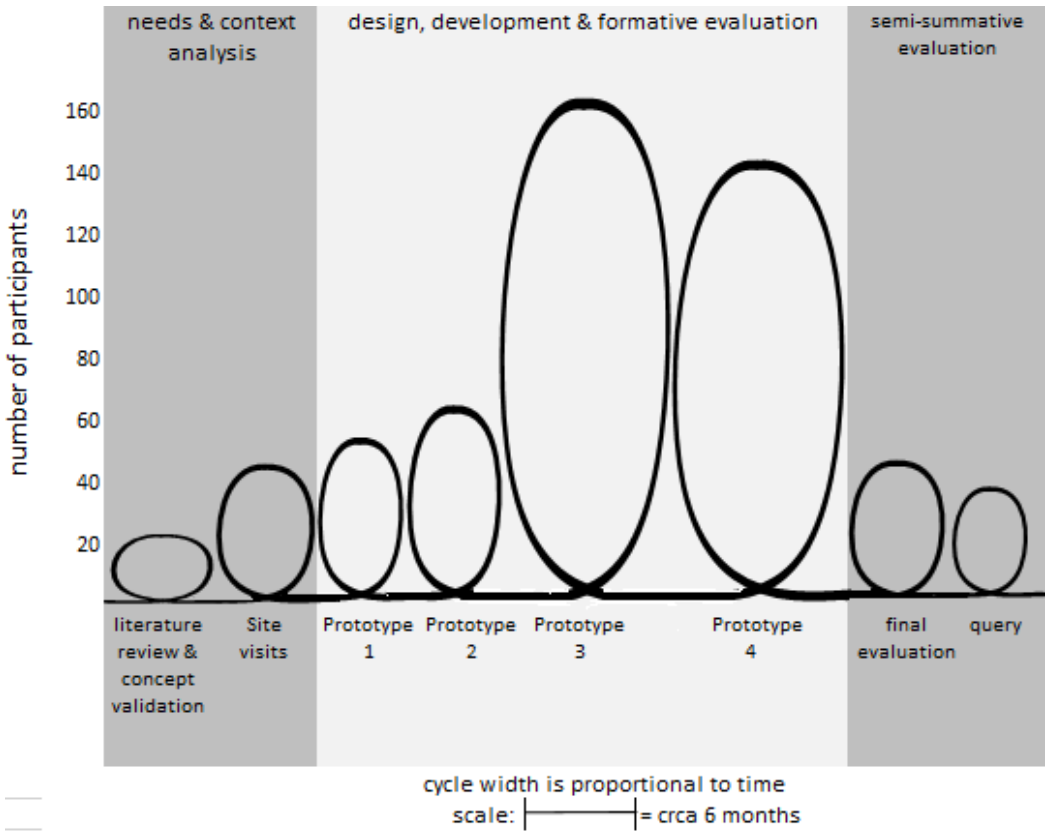


Figure 2-5: Cyclical approach to the three phases followed in the evaluation of the CASCADE-SEA program (Mckenney & van den Akker, 2005:49)

The evaluation of the CASCADE-SEA program made use of the following six related instruments to gather data:

a) interview and walk-through schemes;
b) questionnaires;
c) discussion guides;
d) observation and demonstration schemes;
e) logbooks; and
f) document analysis checklists.

Across the three phases of the research project, four basic strategies were used during the data collection phase: (a) screening, (b) expert appraisal, (c) micro-evaluation, and (d) try-out. Mckenney and van den Akker (2005:49) indicated that the strategies were used as follows:

(a) The screenings were performed by the developers with the intent of providing a comparison of the developed artefact against the artefact's intended quality aspect;

(b) During the expert appraisals, the experts provided feedback regarding the range of already developed artefacts that ranged from conceptual designs to working prototypes;

(c) During the micro-evaluation, the prototypes were evaluated with relatively small groups of experts and users who fell out of the bounds of the intended setting;

(d) Lastly, the try-out allowed the prototype artefact to be tested by the target user group within its target setting.

"Participants in the four strategies belonged to user groups (preservice teachers, in-service teachers, or curriculum developers) and/or expert groups (science education, curriculum development, or computer-based performance support experts)" (Mckenney & van den Akker, 2005:50). The completion of a data circuit was as a result of one of the four strategies being used. Table 2-14 below provides a summarised view of the thirty three circuits that occurred as part of the three phases, namely being the *needs analysis* for the particular context, the *design, development and formative evaluation* (formative evaluation is referred as testing within this study) of the artefact, and lastly the *semi-summative evaluation* (referred to as the summative evaluation in this study).

Table 2-14: Research activities overview (Mckenney & van den Akker, 2005:51)

Phase	Cycle	Circuit	Strategy				Participants						#
							Users			Experts			
			DS	*EA*	*ME*	*TO*	*PS*	*IS*	*CD*	*SE*	*CD*	*PS*	
Needs and context analysis	*Literature review & concept validation*	1											5
		2											5
		3											3
		4											5
	Site visits (discussion tool)	5											24
		6											27
		7											3
Design, development, and formative evaluation of prototypes	*Prototype 1*	8											4
		9											15
		10											19
		11											12
	Prototype 2	12											4
		13											25
		14											34
	Prototype 3	15											4
		16											12
		17											3
		18											10
		19											33
		20											18

		21											19
		22											18
		23											30
		24											22
	Prototype 4	25											4
		26											11
		27											11
		28											44
		29											54
		30											16
Semi-summative evaluation	*Final evaluation*	31											19
		32											17
		33											9
	Query	34											34
Totals:			**4**	**14**	**10**	**6**	**6**	**13**	**13**	**23**	**26**	**12**	**573**
Estimated total respondents when corrected for those who participated more than once:													**510**

Legend = Strategies used = Types of respondents

Strategies: DS=developer screening; EA=expert appraisal; ME=micro-evaluation; TO=try-out
Users: PS=preservice teachers; IS-in-service teachers; CD=curriculum development
Experts: SE=science education; CD=curriculum development; PS=performance support

The data analysis phase required that the collected data be analysed and classified according to its quality criteria (i.e. its *validity*, *practicality*, and *impact potential*). Each circuit in the research process was evaluated for the weight of its data, which was rated twice. The first represented the perception of the researcher before the initiation of each circuit, and the second represented the perception of the researcher after every activity had been performed.

A similar study conducted by Heymann and Greeff (2018:16) portrays the cyclical and iterative approach as specified in the Mckenney and van den Akker (2005:49) study on the evaluation of the CASCADE-SEA program. Three phases of (a) needs-context analysis, (b) design-formative evaluation of prototype tools, and (c) a summative assessment were followed for three cycles through an agile development methodology approach.

The seven DSR guidelines specified in Section 2.4.3 have been accepted as integral to high quality DSR output, and researchers have often requested a more specific set of checklist questions that could be used to evaluate a DSR project. Table 2-15 provides just such a checklist of questions that can be used to communicate the success of a research project. It is important to note that this section of the study specifically relates to guideline number 7, *communication of research,* of Hevner *et al.* (2004:90).

Table 2-15: Design science research checklist (Hevner *et al.*, 2004:20)

Questions
1. What is the research question (design requirements)?
2. What is the artefact? How is the artefact represented?
3. What design processes (search heuristics) will be used to build the artefact?
4. How are the artefact and the design processes grounded by the knowledge base? What, if any, theories support the artefact design and the design process?
5. What evaluations are performed during the internal design cycles? What design improvements are identified during each design cycle?
6. How is the artefact introduced into the application environment and how is it field tested? What metrics are used to demonstrate artefact utility and improvement over previous artefacts?
7. What new knowledge is added to the knowledge base and in what form (e.g. peer-reviewed literature, meta-artefacts, new theory, new method)?
8. Has the research question been satisfactorily addressed?

Figure 2-6 maps the eight questions specified in Table 2-15 to the DSR cycles by Hevner (2007:2), which were discussed in Section 2.4.1.3. The figure demonstrates the relationship of the questions to the cycle to which they are most relevant.

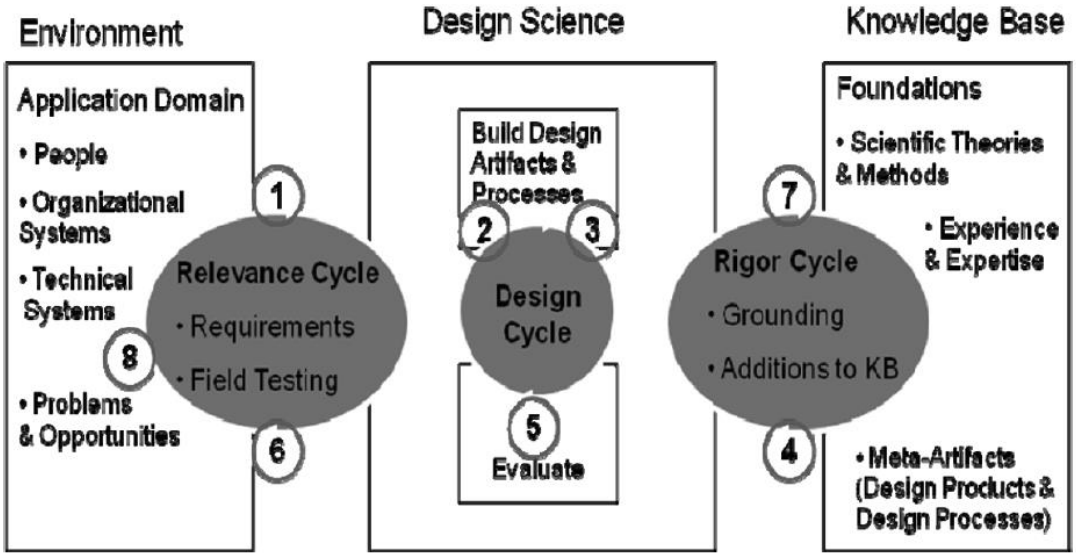


Figure 2-6: A mapping of the eight checklist questions to the three design research cycles (Hevner *et al.*, 2004:20)

The section that follows will discuss the general ethical considerations for performing DSR research.

2.4.5 Ethics in design science research

Ethics can be viewed as the moral principles that influence or govern moral behaviour. Myers and Venable (2014:802) suggest four reasons for considering DSR ethical principles for a study: (1) the dual potential of information technology (IT), which shows how IT can improve lives or destroy people's dignity, (2) increased attention to teaching ethics in business schools, as there is a recognition for more stringent requirements for ethics in this faculty, (3) increased focus by institutional review boards on ethical principles on ethics followed in research projects, and (4) the differing ethical priorities required by DS researchers as compared to behavioural researchers in IS.

Myers and Venable (2014:803) specify a set of six ethical principles that can be used for design science in information systems, which are derived from: (1) Mason's four ethical issues for the information age that refer to privacy, accuracy, property, and access of information, (2) ethical principles considered by institutional review boards for research involving human subjects, (3) the principles specified by the Association of Computing Machinery (ACM) Software Engineering Code of Ethics and Professional Practice, and (4) Venable's critical system heuristic framework to design science research. It is important to note that the six ethical principles summarised in Table 2-16 should not be applied mechanistically, but should be well thought out as to how they will be used by the researcher in a research endeavour.

Table 2-16: Proposed set of ethical principles for design science research (Myers & Venable, 2014:806)

	Ethical principle	Description
1	public interest	All stakeholders who will explicitly be affected need to be identified by the design science researchers and the harm or benefits that may result needs also be considered.
2	Informed consent	Informed consent needs to be obtained from all the participants who are involved in the design science research.
3	Privacy	The design science researchers should ensure all the necessary protection mechanisms are in place to protect the privacy of the participants as well as the privacy of all individuals who may be impacted by the artefact in the future.
4	Honesty and accuracy	The design science researchers must honestly and truthfully report on the findings from the research as well as not plagiarise any ideas. Inspiration obtained from other sources needs to be acknowledged. Design science researchers should not plagiarise ideas, but should acknowledge inspiration from other sources. They should also honestly report their research findings about the new artefact.
5	Property	Intellectual property (IP) should be agreed upon at the start of the research, including any ownership and rights for the information which is collected during the research project.

	Ethical principle	Description
6	Quality of the artefact	The quality of the artefact should be of high importance. A risk-based approach should be taken for the evaluation and testing of the artefact. This will ensure the artefact is safe when used and can be tested rigorously in its environment.

It is important that the researcher considers which of these specific principles are applicable and which group of people may be impacted by the study. This consideration is typically made during the problem identification or before building the artefact. Additionally, ethical awareness needs to be maintained by the researcher throughout the research project.

Ethics are important in preventing research misconduct. Research misconduct implies a) *fabrication*, which entails the false generation of data or results and then recording them as part of the research findings; b) *falsification*, which entails the manipulation of the research components or omitting data in order to produce inaccurate representations; and c) *plagiarism*, which entails using another researcher's results without giving them credit where it's due.

The section that follows will discuss design science research as it pertains to this study.

2.5 DSR in this study

Design science research in terms of how it relates to this study is explained.

2.5.1 DSR frameworks used in this study

The design science research frameworks that are specifically used in this study are explained in terms of how they are used to address the research objectives.

2.5.1.1 DSRM process model: Research objectives

With a better understanding of design science research, the research objectives of this study can be defined within context of the developmental nature of the DSR process model. It is for this reason that the research is restructured to align with the DSRM process model by Peffers *et al.* (2007:54). The objectives of this study are aligned to the DSRM process as summarised in Table 2-17.

Table 2-17: Research objectives of this study aligned to the DSRM process model

DSR process	Objectives
Problem identification and motivation	**Theoretical objectives** • To identify the research problem. • To motivate the process for conducting the research. • To determine the required fields of research to inform a solution for the research problem.
Objectives of a solution	**Theoretical objectives** • To create a shared understanding of design science research. • To understand the concepts of cyber-security and the area of social engineering within cyber-security. • To identify what artefacts are available to raise cyber-security and social engineering awareness in particular.
	Empirical objectives • Present findings from the literature in a participatory design workshop. • Analyse the feedback received from the requirements gathered during the participatory design workshops. • Develop and present a conceptual design as a solution to the problem that is based on the requirements gathered from the target users.
Design and development	**Theoretical objective** • To form a conceptual link between design science research and the feedback analysed from the data obtained during the requirements analysis.
	Empirical objectives • To design and develop an artefact that meets the design and functionality requirements obtained from the requirements analysis. • To develop the artefact through an iterative approach until a usable prototype is reached.
Demonstration	**Theoretical objectives** • To explain how the requirements analysis and literature informed the design process through the use of artefact screenshots coupled with explanations.
	Empirical objectives • To demonstrate the artefact to the target audience.

DSR process	Objectives
	• To continuously evaluate the results obtained from the iterative demonstration of the artefact and determine any notable responses for future research at the end of the development prototype.
Evaluation	**Theoretical objective** • To determine a suitable reporting method for the feedback received from the summative evaluation and testing of the artefact.
	Empirical objectives • To conduct a reaction evaluation with participants from the target audience as part of the evaluation of the artefact. • To conduct a learning evaluation with participants from the target audience as part of the evaluation of the artefact. • To analyse the feedback obtained from the reaction evaluation using qualitative data analysis techniques. • To analyse the feedback obtained from the learning evaluation using quantitative data analysis techniques. • To evaluate the quality of the artefact against a quality evaluation criteria.
Communication	**Theoretical objectives** • To communicate the design science research approach followed developing an artefact for raising social engineering awareness among administrative staff. • To communicate limitations within the context of the study by reflecting on restrictions of the research. • To communicate the reflections on the study recommendations for further improvement of the artefact in future research.

2.5.1.2 DSR cycles: Guiding the artefact development process

For this study, the DSR cycles by Hevner (2007:2) were explained in Section 2.4.1.3. The DSR cycles are used to inform the development of the artefact. A discussion of this process will follow in each chapter where the cycles are used. This will structure the respective chapters that form part of the prototype design and development process.

2.5.2 Design evaluation

The evaluation of the artefact designed in this study is explained. To provide perspective, it is important to note that the artefact final evaluation was intended to occur in the form of a participatory design workshop, but due to the COVID-19 pandemic, the evaluation was performed

electronically as a summative evaluation and test which occurred over two sessions as opposed to the planned singular participatory design session. The two sessions address the ***learning*** evaluation and ***reaction*** evaluation as per the four-level evaluation model by Petri and von Wangenheim (2016:995), which was discussed in Section 2.4.2.

2.5.2.1 Participants

The main participants relevant to this study fall within the demographic of end-users employed in administrative roles within medium to large organisations. The demographics of the participants are selected particularly because the roles they are employed in allow them to have access to sensitive information within their respective organisations. The sensitive information is information such as finances and internal contacts. In many instances, these delegates also initiate or approve workflows within business critical systems, which means that they pose a higher information security risk to the organisation.

Even though this research study is primarily focused on end-users employed in administrative roles within a medium to large organisation (which we will refer to as the target user participants), it is imperative to note that research experts from academia, a design artist, as well as a cyber-security expert and cyber-security professionals were involved in the study as participants. A total of 27 unique participants were involved in this study. Four experts were involved (see Appendix D for participatory design), two of whom were design experts (referred to as E1 and E2 in Appendix D), one a cyber-security expert (referred to as E3 in Appendix D), and another was a design artist (referred to as E4 in Appendix D), all of who provided expert guidance on the design elements of the artefact. Four target user participants (referred to as P1 to P4 in Appendix D) from Company A (academic institution) provided design input that was used to develop a suitable artefact. The four target user participants (P1 to P4) all formed part of the ***reaction*** evaluation (the ***reaction*** evaluation participants are referred to as RP1 to RP4 in Appendix D) during the *summative evaluation and testing* of the developed artefact. An additional four target user participants from Company B (corporate institution) also provided design input (during a workshop) that was used to develop the artefact. Two of the four participants from Company B formed part of the target user participants (as administrative staff and are referred to as P5 and P6 in Appendix D) and the remaining two were cyber-security professionals (referred to as P7 and P8 in Appendix D). Fifteen unique target user participants were part of the ***learning*** evaluation during the *summative evaluation and testing*. The fifteen unique target user participants are from Company B and are refer to as LP1 to LP15 in Appendix D. A summary of the number participants involved in the participatory design is depicted at the end of Appendix D.

2.5.2.2 Data gathering and analysis methods

Data is gathered from the participants in separate participatory design workshops. Five participatory design workshops were planned for gathering the data and only three were performed. The three workshops performed were for gathering the design requirements for developing the artefact as well as for testing it where applicable. Two additional participatory design workshops were planned for gathering data on the *summative evaluation and testing* of the artefact (as the ***reaction*** and ***learning*** evaluation), but due to the COVID-19 pandemic, the *summative evaluation and testing* was performed electronically. For the *summative evaluation and testing*, questionnaires were delivered to the respective participants using Google forms as an online delivery platform. The electronic forms were delivered as two separate data gathering approaches, one for the ***reaction*** evaluation (which gathered qualitative data) and the other for the ***learning*** evaluation (which gathered pre- and post-test data).

The qualitative data gathered from the feedback in the workshops with the participants is analysed using open coding. Open coding is used to identify themes and codes in the qualitative data. These themes and codes are tabulated and utilised as a guideline to develop the artefact (refer to Section 7.3.1 for the ***reaction*** evaluation results).

The pre- and post-test is performed to evaluate the usefulness of the artefact. The data gathered in the evaluation is pre- and post-test scores from a set of questions presented to the participants. These questions are presented to the participants before they would have had an opportunity to interact with the artefact. The questions (as the pre-test) would rate the scale of awareness that the participants currently have regarding social engineering issues.

The artefact is then presented to the participants, which is followed by another set of questions (as the post-test). The artefact will inform the participants regarding concepts pertaining to social engineering issues (refer to Section 6.2 for the social engineering concepts depicted in the artefact). The questions presented in the pre- and post-test questionnaire are identical for the purpose of being able to accurately measure and compare the results. Inferences are made by comparing the results of the second questionnaire (post-test) to those of the first questionnaire (pre-test). From the comparison, it will be possible to determine whether the participants have obtained an enhanced understanding of the concepts pertaining to social engineering. If the participants are able to answer more questions correctly in the second questionnaire, it implies that awareness regarding social engineering has been raised after interacting with the artefact (refer to Section 7.3.2 for the pre- and post-test ***learning*** evaluation results).

2.5.3 DSR guidelines followed

The research guidelines followed in this study are from the seven guidelines by Hevner *et al.* (2004:83), which were discussed in Section 2.4.3. The DSR guidelines that guide this research approach are explained.

Guideline 1: Design as an artefact

The artefact design and development is informed by the participants and the problem relevance. The literature informs the approach for designing the artefact (Hevner *et al.*, 2004:83).

Guideline 2: Problem relevance

The relevance of the research problem is informed by the literature. The literature specifies that a problem is experienced by users of information technology regarding social engineering issues. The literature also indicates a gap in the research knowledge base, which consequently informs the necessity for this study.

Guideline 3: Design evaluation

This study produces a design science research artefact that has its design informed by the cyclical approach prescribed by Hevner (2007:2). The design cycle ensures that the artefact is continuously evaluated throughout its design.

Guideline 4: Research contributions

Research contributions are noted throughout the research process. The contributions are communicated through each cycle that the DSR study goes through. The research knowledge base is consulted and any new knowledge contributions are communicated.

Guideline 5: Research rigor

The artefact design is rooted in the DSR cycles by Hevner (2007:2). The research objectives of this study are structured according to the six guidelines of the DSRM process model by Peffers *et al.* (2007:54). Open coding is used to analyse the qualitative data (Romand Jr *et al.*, 2003:222). The artefact's effectiveness is measured using pre- and post-testing (Jerry Chih-Yuan *et al.*, 2017:48).

Guideline 6: Design as a search process

The artefact is designed over several iterations per the cycles by Hevner (2007:2), which is indicative of a search process.

Guideline 7: Communication of research

The theoretical component of the study is informed by the six activities of the DSRM process model by Peffers *et al.* (2007:52). An approach similar to that followed by Mckenney and van den Akker (2005:49) guides the reporting of the artefact. The final chapter in this research document communicates the results of the research which includes the use of the DSR checklist by Hevner and Chatterjee (2010a:20) to evaluate whether the study followed the appropriate steps to satisfy the research question.

2.5.4 Reporting on this DSR study

The reporting of this DSR study follows a similar style to the way in which Mckenney and van den Akker (2005:49) reported on their evaluation of the CASCADE-SEA program. As a practical example of how this reporting style will be performed, the study by Heymann and Greeff (2018), as illustrated in Figure 2-7, is referred to.

In the first phase (needs & context analysis), a literature review is performed to ground the research. A needs analysis is performed to identify the need for performing the research and how that need would be satisfied. The requirements are gathered and subsequently translated into the development of a conceptual design that is further validated by the target audience.

In the second phase (design, development, and formative evaluation), a prototype is designed through a cyclical approach whereby the design requirements and the prototype design are iteratively improved and evaluated until a suitable design is reached and evaluated through an evaluation process.

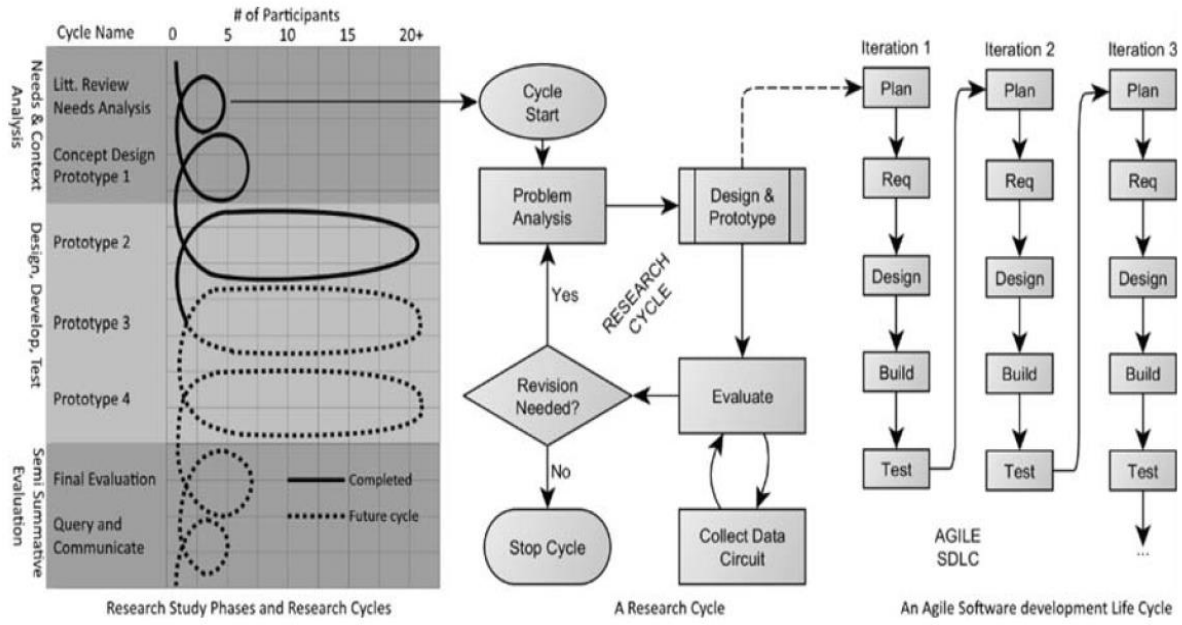


Figure 2-7: The Mckenney and van den Akker (2005:49) research cycles as followed by Heymann and Greeff (2018:16)

In the final phase (summative evaluation and testing), the final prototype design is tested and the results of the testing are summarised and communicated.

The design science research checklist (see Table 2-15) by Hevner and Chatterjee (2010a:20) is used to evaluate whether this study has adequately addressed the important aspects of a design science research study.

2.5.5 DSR ethical considerations for this research

The DSR ethical considerations for this research are informed by the proposed set of ethical principles for design science research as described by Myers and Venable (2014:806) which are:

The public interest

The participants who are relevant to the study are identified. The participants were identified as administrative staff employed in medium to large organisations. The impact of the research and how these factors will affect the participants are clearly understood and defined. The participants are informed electronically through email as well as in person as part of the explanation of the consent forms on how this research will affect them and why they should take an interest in it.

Informed consent

Informed consent is obtained from all the participants of this study through consent forms, which clearly describe the objectives of the research and what is expected from the researcher and participants (refer to Appendix C for consent form template). Ethical clearance is obtained from the university where the research takes place, to ensure that the risks of the research are within the boundaries of ethical requirements for this type of research (refer to Appendix B for ethical clearance form).

Privacy

Any information that is obtained from the participants is treated anonymously. Any confidential information is redacted to ensure that the participants cannot be identified. Any information obtained that may potentially be linked to a participant or group of participants is securely stored only for the duration of the study and will be removed immediately after.

Honesty and accuracy

All information is presented with honesty and accuracy as required by the NWU research code of conduct (refer to Appendix A). The information is not to be altered in any way as to obscure the truth of the outcomes. All the information is captured and recorded accurately to ensure that the research performed reflects the truth.

Property

As part of the informed consent, the participants are informed about the ownership of intellectual property. The researcher is aware of the intellectual property of all inferences and contributions of the research. The research outputs will remain the property of the North-West University as described in the management of intellectual property at the NWU policy document (North-West University, 2010:12).

Quality of the artefact

The quality of the artefact is addressed through participatory design workshops during which end-users from the target user group provide design feedback and test the artefact. It is also iteratively tested over multiple test and feedback sessions by the research experts and a design artist.

2.6 Conclusion

In this chapter, the research paradigms that can be employed for information systems-based research were examined (in Section 2.2). Their associated methodologies, frameworks, and

methods were also discussed. The paradigms were positivism, interpretivism, critical social theory, and design science research. Positivism (Section 2.2.1) is a scientific paradigm that assumes that the independent facts regarding a single perceivable reality can be quantitatively measured. Interpretivism (Section 2.2.2) focuses on human interpretations and meanings of the world they interact with. Critical social theory (Section 2.2.3) aims to emancipate individuals and groups into an equal society. Design science research (Section 2.2.4) seeks to create unique artefacts as a way to enhance and comprehend the features and behaviours of information systems.

The study was positioned in the design science research paradigm (discussed in Section 2.2.5). This was primarily due to the primary objective of the study requiring the development of a novel artefact. The design science research paradigm was discussed in detail (in Section 2.4), elaborating on the data analysis techniques and frameworks that can be employed within the paradigm. The frameworks discussed were the design science research process model by Vaishnavi *et al.* (2004/2019:8), the design science research methodology process model by Peffers *et al.* (2007:54), and the design science research cycles by Hevner (2007:2).

The design evaluation guidelines for developing and evaluating a quality artefact were also described. The evaluation guidelines discussed the main participants that are relevant to this study and how they will selected, identified, and allowed to provide rich data for the study. The data gathering and analysis methods for the study were also discussed which defined how participatory design workshop data would be collected and analysed as well as how the artefact evaluation and testing data would be collected and analysed.

The research guidelines described in the seven guidelines by Hevner *et al.* (2004:83) were discussed in Section 2.5.3. The approach that would be employed in the reporting of this study was also described in Section 2.5.4 which followed an approach similar to that of Mckenney and van den Akker (2005:49) as was used in the study by Heymann and Greeff (2018:16). Ethical considerations for conducting ethical research were lastly discussed in Section 2.5.5.

The chapter that follows will discuss the literature that is relevant to this study. The chapter will specifically discuss cyber security, social engineering as a concept in cyber security, and the types of artefacts available for raising awareness regarding cyber security and social engineering issues.

CHAPTER 3: LITERATURE REVIEW

3.1 Introductions

The primary objective of this study is to design and develop an artefact that can be used to raise awareness about social engineering attacks among administrative staff in medium to large organisations. This chapter will support this primary objective by creating a shared understanding of cyber-security, by providing an overview of the different cyber-security issues and then further discussing social engineering. This chapter will also briefly describe artefacts that have been developed to raise awareness about social engineering.

Cyber-security is a term that defines the methods, processes, and technologies within the context of information systems that aim to protect the programs, applications, networks, computers, and data contained and transmitted by these systems from being compromised by an attacker (Jain & Pal, 2017:791). Cyber-security looks at the major areas pertaining to application security, information security, e-mail security, mobile device security, web security, and wireless security. The general aim of cyber security is to maintain the confidentiality, integrity, and availability (CIA) of data (von Solms & van Niekerk, 2013:98).

There are several definitions of cyber-attacks in international literature, all of which lead to the same conclusion. A cyber-attack is described by Kim *et al.* (2014:489) and Bendovschi (2015:25) as an act of deliberate exploitation of computer systems, technology, and network components with the goal of compromising the confidentiality, integrity, and availability of data.

More formally (from an international point of view), in 2011, published in a lexicon for military use within cyber-operations, the Joint Chiefs of Staff defined a cyber-attack as (The joint chiefs of staff, 2011):

*"*a *hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber-attack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 (command and control) capability. A cyber-attack may use intermediate delivery vehicles, including peripheral devices, electronic transmitters, embedded code, or human operators*".

Cyber-attacks are possible because of threats and vulnerabilities. A threat, within the context of information systems, is viewed as the possibility to exploit a vulnerability, intentionally or unintentionally, in order to compromise or damage an information system asset. A vulnerability is an information system security weakness that could potentially be exploited to gain unauthorised

access to confidential information (von Solms & van Niekerk, 2013:100). Kafol and Bregar (2017:82) recognise that cyber-attacks are rapidly on the rise on a global scale and that cyber-criminals are getting better in the methods and techniques used to successfully perform these attacks. According to Croock (2016), South Africa is ranked as the country with the highest financial and cyber-crime risk across the Sub-Saharan African states, making it the country suffering from the highest number of cyber-attacks in the region. This is primarily as a result of its rapid economic development within the African region and the lack of skills to accommodate this rapid development. These attacks have gradually steered away from the exploitation of information technology infrastructure, to a greater focus on people. People are considered the weakest link within an organisation's cyber security (Aldawood & Skinner, 2018:62). The most commonly attacked industries are military, energy, the financial sector, and critical infrastructure installations. Cyber-attacks may be carried out in a variety of means, ranging from hacking, bombing, cutting, infecting, etc., with the primary aim of disrupting computer network operations (Hathaway *et al.*, 2012:826). They can be carried out on information technology through viruses and malware, or on people through social engineering and cyber bullying (Aldawood & Skinner, 2018:62).

A vulnerability is a weakness or bug found within the implementation or design of an application (Jain & Pal, 2017:711). It creates a potential system risk that can be used by an attacker to exploit the system and gain unauthorised access to information. A software exploit is a piece of code or program that takes advantage of a vulnerability and enables an attacker to gain access to computational resources in order to perform malicious activity or steal sensitive information (Wolf & Fresco, 2016:269). Software exploits are malicious code vulnerabilities that are known to the public, whereas zero-day exploits are not. A zero-day exploit is a system vulnerability that has not yet been disclosed to the vendor and is not known to the public (Ciancioso *et al.*, 2018:663). Attackers use these zero-day exploits on system vulnerabilities to gain access to the network environment in order to perform malicious actions or steal information (Sood & Enbody, 2014:1). What makes zero-day exploits so dangerous is that they are not known to the software vendor and therefore do not have a patch developed to remediate the *potential* vulnerability. These zero-day exploits can easily be purchased using cryptocurrency on the black market (dark web) of the Internet and would typically not require specialist skills to utilise, once obtained (Kirkpatrick, 2017:22).

Cyber-attacks have multiple classifications based on the attacker and victim's point of view. A study by van Heerden *et al.* (2012), as referenced by van Heerden *et al.* (2016), provides a description of these classifications within the context of computer network attacks. These classifications are dissected in the study by Myers and Venable (2014:802), who classify them as

having an attacker, goal, mechanism, effect, motivation, target, vulnerability, and scenario. Definitions of these classifications are summarised in Table 3-1. Each of these classifications were further divided into three sub-classes.

Table 3-1: Summary of cyber-attack classes and their respective sub-classes (van Heerden *et al.*, 2016:2)

Classification	Description	Sub-classes
Attacker	The attacker (also known as hacker, cracker, fraudster, conman, or aggressor) describes the entity that is performing the attack.	The attacker class consists of the following subclasses: hacker, insider, or criminal.
Goal	Goal refers to the purpose of the attack.	Divided into the following subclasses: stealing, disrupting, or changing data (CIA).
Mechanism	Mechanism represents the attack methodology.	The subclasses include: denial of service, system abuse, and information gathering.
Effect	Effect of the cyber-attack can be described as the recoverability of the damage.	Effect can be classified as: minor, major, or critical.
Motivation	Motivation refers to the primary reason or motive of the attack.	The motivation for a cyber-attack can be one of the following: political, criminal, financial, or personal.
Target	Target refers to the physical devices that are targeted by a cyber-attack.	These include: computer systems, mobile devices, or network infrastructure.
Vulnerability	Vulnerability refers to the technical weakness exploited by the attacker.	The following common subclasses are applicable: configuration, design, and human weakness.
Scenario	Scenario refers to the situations of cyber-attacks.	These scenarios are typically used to classify cyber-attacks: denial of service, web defacement, and unauthorised access.

van Heerden *et al.* (2016:4) provide a timeline of some of the most notable cyber-attacks that have occurred (within the context of South African organisations) between 1994 and 2015. This timeline is summarised in Table 3-2. These attacks pertain to the classifications specified in Table 3-1.

Table 3-2: Summary of cyber-attacks that have occurred in South Africa from 1994 to 2015 (van Heerden *et al.*, 2016:4)

Date and victim	Attack description
1994: SA Election	An attempt was made by an unknown hacker to sabotage the Election Commission's electorate results on 3 May 1994.
1998: Telkom	Telkom was hacked on 22 October 1998 by a 15-year-old.
1999: SA Statistics	A defacement of the South African statistic web site.

2003: ABSA Bank	An attacker sent emails containing spyware to ABSA clients. The attacker used the phishing emails to obtain personal identification numbers (PIN) of customers and stole more than R530 000 from the customer bank accounts.
2005: Mass Defacement	The Team Evil hacker group from Morocco defaced more than 260 South African websites. It was deemed the biggest cyber hack in South Africa's history.
2010: LandBank	Attackers attempted to hack LandBank and steal R150 million. Insider threats were used to obtain the information technology system's passwords.
2011: Spyphone	A businessman performed a man-in-the-middle attack on his wife to intercept email, SMS, and other electronic communication. He then used this information against his wife during the divorce proceedings.
2011: ANCYL	Between the period March 2011 and August 2011, the African National Congress Youth League's (ANCYL) web site was defaced multiple times.
2012: PostBank	R42 million was stolen by a hacker who hacked the South African PostBank.
2013: IOL DDoS	The hacker group 'Anonymous Africa' launched a Distributed Denial of Service (DDoS) attack against the Independent Newspaper website iol.co.za.
2014: Mr Price	A conman attempted to access the clothing account of a Mr Price customer.
2015: State Security Agency Spy Cables	Leaked information was obtained from the South African State Security Agency (SASSA) by the Al Jazeera news agency between 2006 and 2014.

In an incident that occurred mid-year of 2016 at the University of Limpopo, the hacktivist group known as *Anonymous,* hacked the University's IT infrastructure and conducted a web defacement attack on the University's home page. The hacktivist group claimed that the University's web server admin had limited knowledge on what a vulnerability was and suggested that the administrators review its security controls (Anonymous, 2016). Figure 3-1 depicts the message left by the hackers on the defaced university site.

In another incident that occurred at the University of Cape Town on 2 July 2003, a hacker who went by the name *h4ck3rsBr* conducted a web defacement attack on the University's IT services website (Lombard, 2003).

The trends are similar on an international scale. Krombholz *et al.* (2015:114) recognise social engineering as an emerging threat that has been used to compromise large multinational corporations and news agencies. These entities had fallen victim to social engineering attacks. These corporations include Google (2009), Rivest Shamir and Adleman (RSA) (2011), Facebook (2013), as well as the New York Times (2013). Table 3-3 provides a summary of the organisations that were compromised. The table depicts the year the compromise occurred and the type of social engineering attack vector used.

Figure 3-1: Web defacement attack on the University of Limpopo web page (Anonymous, 2016)

Table 3-3: Social engineering attacks on large multinational corporations

Organisation	Year	Vector	Attack description
Rivest Shamir and Adleman (RSA)	2011	Advanced persistent threat (APT): Spear phishing	An Adobe Flash Player vulnerability was exploited through an email that contained a spreadsheet with a zero-day exploit. The email was sent to several employees who worked at RSA.
New York Times	2013	APT: Spear phishing	Spear-phishing was used as the attack initial entry point which allowed attackers to gain passwords of 53 employees.
Apple and Facebook	2013	Waterholing	A Java vulnerability was used by attackers to exploit devices that visit the compromised websites. The attackers were then able to pivot onto the corporate networks from the compromised devices.
Twitter	2013	Waterholing	The waterholing attack on twitter followed a similar attack methodology as that used in the Apple and Facebook attack. The only difference was that it was not confirmed exactly which vulnerability was exploited for the initial attack entry point before attackers were able to pivot onto the corporate network.

Based on the cases observed in the literature, it is concerning that South Africa has such a low maturity level to dealing with cyber-attacks. Mimecast, an email security company, published in

its "*third annual state of email security report*" that social engineering attacks were an escalating concern for organisations. The study conducted indicated that 88% of South African respondents had experienced a social engineering attack within the last 12 months, with 53% of the respondents indicating an increase in the number of attacks over the same period (Mimecast, 2019).

The purpose of this chapter is to explore the different categories of issues within cyber security, as well as to briefly discuss some of the attack vectors that could be employed to compromise systems. Additionally, it will briefly discuss how users can be better equipped at protecting themselves from becoming victims of some of these attacks.

3.2 Cyber-security

This section will describe the different categories of issues within cyber-security. The categories are divided into cyber-crime, which deals with small-scale crimes conducted by cyber-criminals who have limited capacity and funding; cyber-terrorism, which is a moderate-scale cyber-crime that is typically funded by large corporations that seek to incite fear in people; and lastly, cyber-warfare, which is a large-scale cyber-crime that is typically funded by state agencies to attack other nations. This section will further discuss social engineering as an attack vector in the cyber-crime domain. Some of the innovations that can be used to raise awareness against these social engineering attacks are also discussed.

3.2.1 Cyber-security issues

Cyber-security issues can be divided into three domains, namely cyber-crime, cyber-warfare and cyber-terrorism. It is important that these issues are understood as they categorise the breadth and width of cyber-security issues that information technology (IT) professionals typically encounter.

3.2.1.1 Cyber-crime

Cyber-crime is an act that is performed by one or more individuals who have the intention of monetary gain, gaining access to confidential information, or intend to cause disruption to services. Within the South African context of the definition of cyber-crime, the Electronic Communications and Transactions Amendment Bill defines cyber-crime as (Pule, 2012):

"any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them."

Kurnava (2016) provides a more complete definition of a cyber-crime by stating:

"*Cyber-crime is a term for any illegal activity that uses a computer, phone, digital notepad, or any other technological device that stores data or uses modern telecommunication networks to commit offences against individuals or groups of individuals. This illegal activity is committed with a criminal motive to intentionally harm the reputation of the victim or cause physical, financial or mental harm or loss, to the victim for personal gain.*"

Some examples of these crimes would be acquiring sensitive information such as credit card details, intellectual property, or even perform a denial of service attack to impair access to a website or other computer resource (Singh & Singh, 2017:2696). Cyber-crime is different from traditional crime, primarily in that cyber-crime is committed through the use of a computing device such as a desktop computer, laptop, mobile device, etc. (Herselman & Warren, 2004:254). It is important to note that almost all kinds of traditional crimes can be performed through the aid of a computing device. These could be crimes such as forgery and fraud, or even murder in the form of a critical device being altered by a hacker, such as illegally changing the junctions of a railway track that could lead to a train accident and loss of life.

A cyber-attack is a cyber-crime that is committed by a non-state actor for a national security or political motive. However, if a cyber-crime is not performed for the aforementioned reasons, but for a personal gain such as intellectual property theft, online fraud, or identity theft, it is then considered cyber-crime (Hathaway *et al.*, 2012:830).

3.2.1.2 Cyber-terrorism

Cyber-terrorism is at an organisational level in that it works independently with the primary aim of performing terrorist activities using the cyber-space as the main platform of attack (Singh & Singh, 2017:2696). It is an act that entails using computer technology to engage in terrorist activity. Although cyber-terrorism and cyber-crime are interlinked, they are not the same thing. Crime, by definition, is motivated by a personal agenda, whereas terrorism is motivated by a political agenda. Acts of cyber terrorism typically aim to instil fear in a group of people or society with the intention of disturbing order and peace (Brenner, 2006:457).

Within the South African context of the definition of cyber-crime, the national cyber-security policy framework (NCPF) defines cyber-terrorism as *(Mahlobo, 2015)*:

"[the] use of Internet based attacks in terrorist activities by individuals and groups, including acts of deliberate large scale disruptions of computer networks, especially computers attached to the Internet, by the means of tools such as computer viruses".

The Department of Homeland Security provides an alternative definition for cyber terrorism, which states that it is (Berinato, 2002):

"*a criminal act perpetrated through computers resulting in violence, death or destruction, and creating terror for the purpose of coercing a government to change its policies*".

3.2.1.3 Cyber-warfare

Cyber-warfare is undertaken at a much larger scale than a cyber-crime, in that it is performed by a nation for espionage against another country, with the primary aim of either obtaining confidential information, or causing service disruption to impair the country's operations and development (Singh & Singh, 2017:2696). Robinson *et al.* (2015:74) elaborate further on the definition of cyber-warfare in that modern warfare does not necessarily aim to advance a national agenda. Cyber-warfare is a term that refers to cyber-attacks that occur in the midst of an armed conflict. There are multiple definitions that are scrutinised by Robinson *et al.* (2015), and it is clear that there is no widely accepted definition of cyber-warfare. However, Brenner (2006:465) makes it clear that cyber-warfare constitutes the conduct of military operations in the cyber-space and that this conduct is likened to that of conventional military force over a competing nation state.

A typical example of cyber-warfare would be the Stuxnet worm. Stuxnet was a computer virus (in the form of a worm) that was designed to infect and affect the operation of supervisory control and data acquisition (SCADA) systems. It was the first known computer network attack that was able to cause physical damage across international boundaries (Lindsay, 2013:1). Stuxnet infects the Windows operating system, typically through a medium such as a flash drive and then propagates over the network (Masood *et al.*, 2011:142). It then exploits zero-day vulnerabilities on the Windows operating system and uses default credentials to access the Siemens programmable logic controllers (PLC) WinCC/PCS 7 programs, which are used to control industrial systems. Stuxnet causes these controllers to behave erratically (Singer, 2015:80). Stuxnet is an example of an advanced persistent threat (APT). APTs are a number of hacking processes that allow an attacker to remain hidden in a system for extended periods, and are directed at specific entities (Al-Rabiaah, 2018:1). With the abbreviation of APT, *advanced* means using advanced exploitation techniques, *persistent* means continuously maintaining access to a system and extracting data, and *threat* means a human contributes in organising the attack.

What categorised Stuxnet as a cyber-warfare attack was that the malware targeted specific centrifuges used in the Iranian Nataz nuclear facility. The facility was suspected of being used in the Iranian nuclear weapons development programme (Singer, 2015:81). Therefore, the attackers were aware of which components the malware would attack and destroy in the facility. More

importantly, the development of Stuxnet would require a big budget to develop as the equipment required to test the malware and the skills required to develop it would come at a substantial cost.

3.2.1.4 Comparing cyber-crime, cyber-warfare and cyber-terrorism

In this section, the difference between cyber-crime, cyber warfare and cyber terrorism is established. The differences between a cyber-attack and cyber-crime are first distinguished for the purpose of clarity.

A cyber-attack typically uses computer or network systems to disrupt or destroy a victim's critical cyber systems. Cyber-attacks usually require the systems that are under attack to have some security flaw in their implementation.

Cyber-crime is generally understood as the means of using a computing device to commit an illegal act. A cyber-crime is defined as "*any crime that is facilitated or committed using a computer, network, or hardware device*" (Gordon & Ford, 2006:14).

Cyber-terrorism, on the other hand, can be described as a cyber-attack that uses or exploits information systems as a means of instilling fear in society as a way of driving a specific ideological objective, or cause damage (Kurnava, 2016).

Cyber-warfare and cyber-terrorism are both rooted in the concept of having a specific target and motivation. However, with cyber-crimes, the primary motive is mainly for self-gain, whereas cyber-terrorism and cyber-warfare have a much wider scope in their motive.

The following section will look at key trends and statistics around cyber-attacks, focusing on the vectors and motivation for the different cyber-attacks.

3.2.2 Cyber-attack vectors and motivation

In this section, the attack vectors and motivations behind cyber-attacks are discussed. The trends on the statistics from 2016 to 2018 indicate that targeted attacks are on the rise (Passeri, 2016). There are a variety of definitions for targeted attacks; however, Sood and Enbody (2014:2) define a targeted attack as "*a class of dedicated attacks that aim at a specific user, company, or organisation to gain access to the critical data in a stealthy manner.*" These attacks seek to compromise a targeted entity while maintaining complete anonymity. Broad-based attacks should be intertwined with targeted attacks, as targeted attacks mainly focus on a variety of users and are random in nature.

In a study by van Niekerk (2017:122) in which cyber incidents that occurred in South Africa between 1994 and 2016 were analysed, it is visible that cyber-attacks have been on the rise in South Africa (Figure 3-2).

Figure 3-3 illustrates the trend behind cyber-attacks in their specific domains between 2016 and 2018. It is clear from the illustration that cyber-crime is the leading motivation behind cyber-attacks.

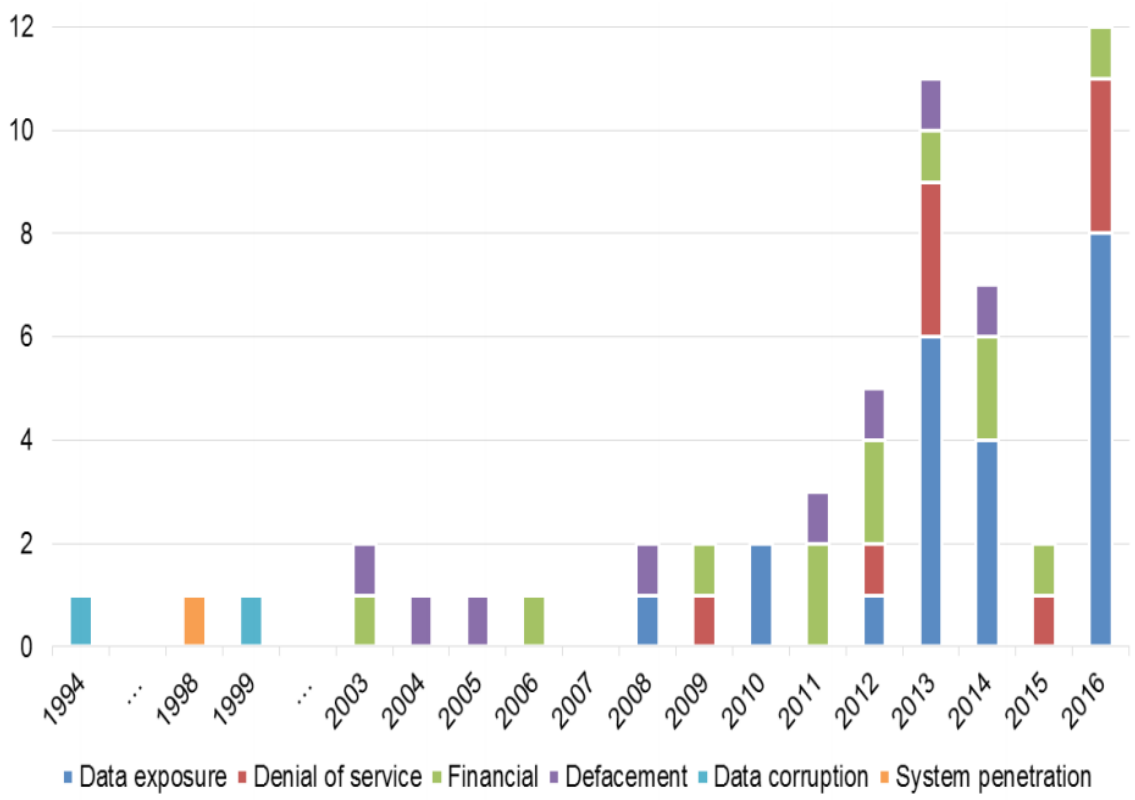


Figure 3-2**: Trend of impacts based on cyber incidents in South Africa (van Niekerk, 2017:122)**

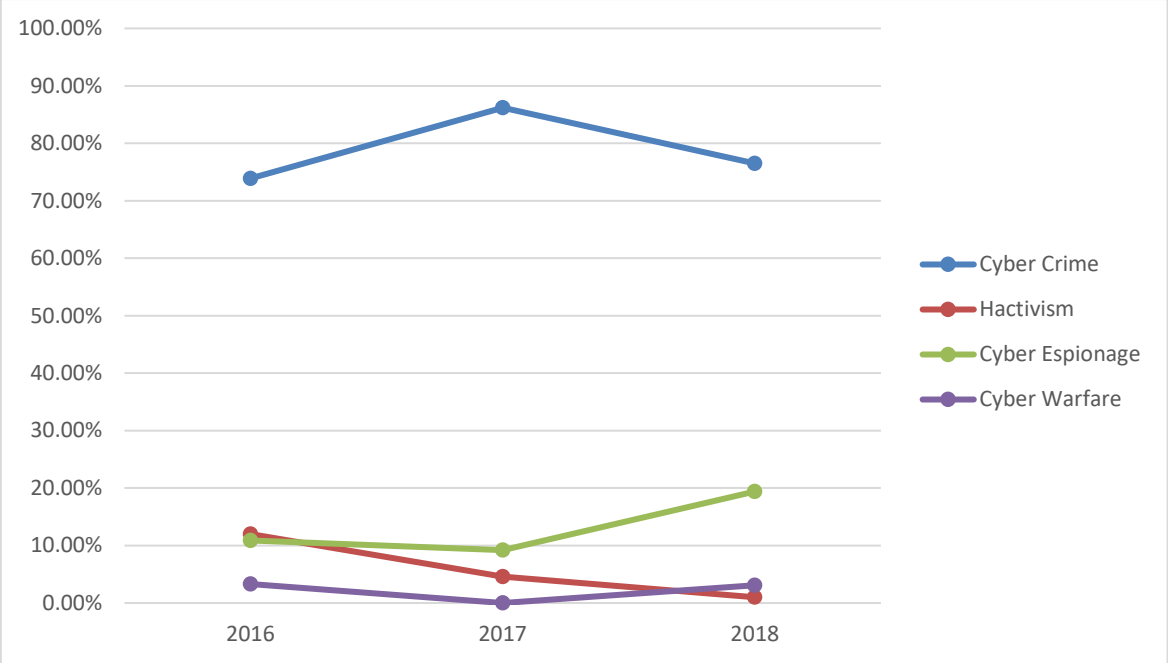


Figure 3-3: Trend showing the motivation behind cyber-attacks between 2016 and 2018 (Passeri, 2016)

The details pertaining to the types of cyber-crime that are employed in cyber-attacks are discussed in the section that follows.

3.2.3 Types of attacks in cyber-crime

This section of the study will look at some of the attack vectors used by cyber actors to compromise the confidentiality, integrity, and availability (CIA) of information systems. Stiawan *et al.* (2017:127) refer to five techniques commonly used by threat actors to gain access to a system; these methods include web implants, malware (viruses), SQL injections, phishing, and password guessing. A sixth common attack is a flooding attack, or otherwise known as denial of service (DoS) attack, prevents users from being able to gain access to a system. These methods are described in Table 3-4 and illustrated in Figure 3-4.

Table 3-4: Cyber-attack techniques (Stiawan *et al.*, 2017:127)

Attack technique	Description
Web implant	These are viruses and other forms of malware that are embedded on a web page. The victim is normally enticed into clicking a web link and the web browser will proceed to secretly install botnets without the user being notified, thereby allowing an attacker to gain access to the system.

Malware	Malware is generally activated when an infected file is clicked by a user, which would typically come from an email attachment or USB flash drive. The installed malware would provide an attacker with a backdoor access to the affected machine.
SQL injection	This process involves an attacker finding a weakness on a web page or back-end system and then injecting malicious queries in the affected systems. An attacker could use this to obtain data and database structures in order to get access to the back-end systems.
Web phishing	Web phishing occurs when an attacker tricks a user into entering valid details and credentials onto a website that appears seemingly legitimate.
Password guessing	Password guessing is when an attacker uses multiple username and password combinations using either a brute force attack or a dictionary attack. Dictionary attacks are performed using a library of commonly used words and phrases to guess a password, whereas a brute force attacks is when every character is sequentially enumerated until a password match occurs.
Flooding (DoS)	Flooding, otherwise known as a denial of service attack, occurs when a target system is overwhelmed with synchronize (SYN) packets without acknowledge (ACK) packets being returned. This effectively causes the system to shut down by reducing bandwidth availability and overloading the servers load capacity.

Figure 3-4 provides a basic illustration of the different stages the above-mentioned cyber-attacks go through during the process of a system compromise.

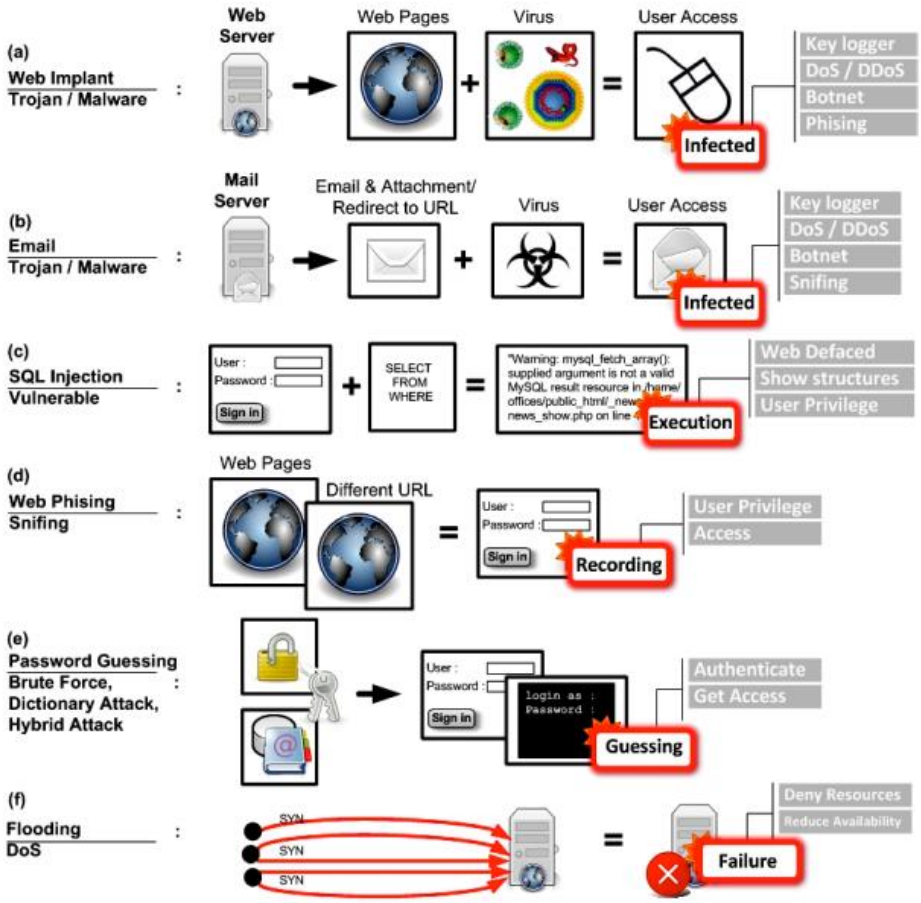


Figure 3-4: Common cyber-attacks and stages of compromise (Stiawan *et al.*, 2017:128)

For the purpose of this study, the above cyber-attacks will be briefly described, with a greater description of social engineering as it is the greatest weakness in the cyber-space realm that is used by most attackers to compromise systems through vulnerabilities in the human element (Heartfield & Loukas, 2015:1).

3.2.3.1 Denial of service attack

Denial of service attacks are typically conducted with the aim of making information system resources unavailable. They are conducted by overloading the system with requests until the system becomes overwhelmed and either becomes extremely slow or crashes. Denial of service attacks are very common, especially with the vast availability of the Internet of Things (IoT) devices. These devices can be compromised by attackers and used to conduct flooding attacks (Jain & Pal, 2017:792). Additional to the denial of service attack is the distributed denial of service attack (DDoS), which occurs when a denial of service (DoS) attack originates from many different computers and network devices (Zhang & Xiao, 2018:1). A simple illustration of a DDoS is

provided in Figure 3-5. The illustration depicts compromised computers (zombies) that are used to launch flooding attacks and cause other devices to become inaccessible.

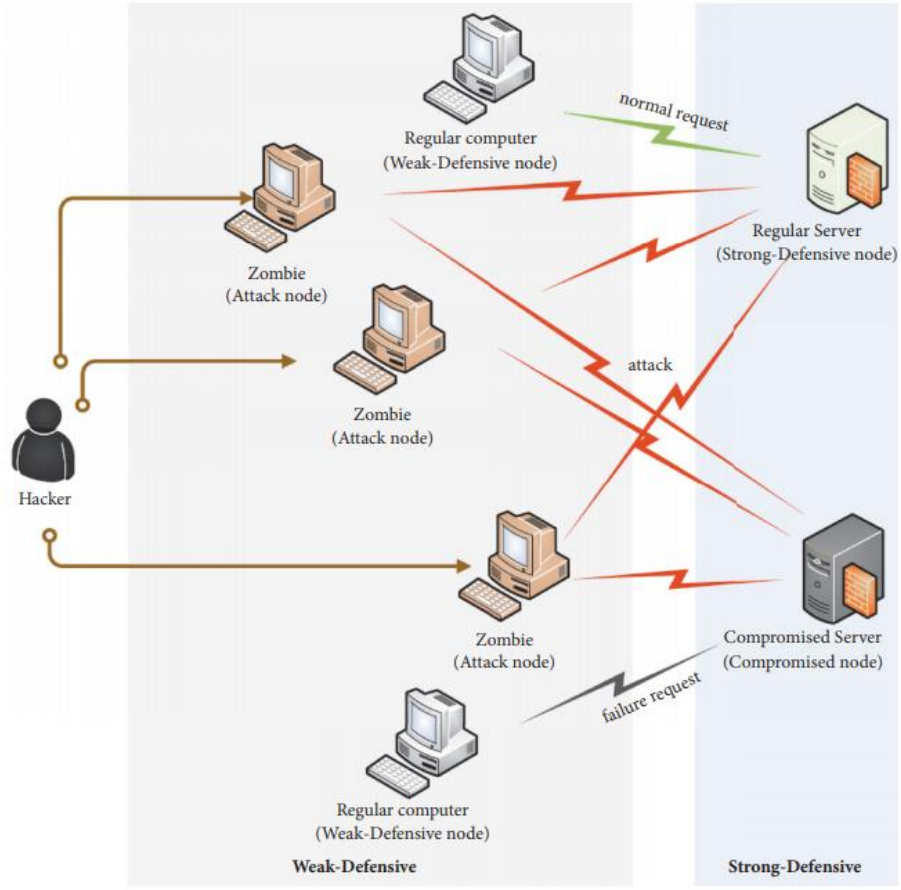


Figure 3-5: Illustration of a distributed denial of service (DDoS) attack (Zhang & Xiao, 2018:2)

3.2.3.2 Password guessing attacks

Password guessing attacks are a technique used by attackers to guess the credentials of a system by trying as many possible combinations of usernames and passwords until the correct combination is matched. These attacks could occur in the form of brute-force attacks, dictionary attacks, lookup tables, or even rainbow tables (Barbieri *et al.*, 2014:1160). One in four network attacks occur through brute forcing techniques (Jain & Pal, 2017:792). There are generally five commonly used password guessing attacks, which are specified in Table 3-5.

Table 3-5: Five most common types of password guessing attacks

Attack type	Attack description
Dictionary attacks	A dictionary attack is when an attacker crafts a list of possible passwords in the hopes that a user will create a password that falls within that domain of commonly used passwords (Pinkas & Sander, 2002:161).
Exhaustive key search	Uses all possible combinations of a character set and ranges of password length.
Reverse brute-force	Using commonly used passwords to login against a list of potential usernames.
Credential stuffing	Credential stuffing attacks occur when an attacker uses automated injection of user credentials (username and password) pairs that have been stolen from a different but compromised website in the hope that a user has re-used those same set of credentials (Wang *et al.*, 2014:513).

3.2.3.3 Browser-based attack

Browser-based attacks are primarily targeted at users who are on the Internet. These attacks trick the user into downloading what seems to be legitimate software, but is in fact malware. The malware will then execute on the victim's system and either cause damage or allow the remote attacker to compromise a victim's system and eventually allow them to access confidential information (Jain & Pal, 2017:792). This disguised malware is often referred to as a Trojan horse (Ab Razak *et al.*, 2016:68).

3.2.3.4 Shellshock attack

Shellshock attacks primarily seek to compromise operating systems such as the Linux Born-again shell (Bash) service (Jain & Pal, 2017:792). Shellshock is a security bug that exploits the bash shell most commonly through Internet facing services such as web servers that rely on the shell to process requests. Shellshock attacks can be launched remotely or from a local machine. The shellshock attack allows an attacker to run arbitrary commands over the network, thereby allowing them to make unauthorised changes to the hosts and compromise sensitive information.

3.2.3.5 SSL attack

Secure socket layer (SSL) attacks occur when an attacker intercepts and decrypts data that is transmitted over a network connection. This is typically due to weak encryption in the SSL being used to encrypt the data on the network connection (Jain & Pal, 2017:792). SSL and transport layer security (TLS) are cryptographic protocols that are used to protect information from being intercepted and read by an attacker who is spying, or eavesdropping, on network

communications. This process of intercepting information in transit is called a man-in-the-middle attack (Fahl *et al.*, 2012:51).

3.2.3.6 Backdoor attack

Backdoor attacks are used to bypass authentication mechanisms on the system in order to gain remote access. These types of attacks are embedded in programs and can be remotely started up by an attacker at any time. These attacks are less common and require very specialised skills to perform (Jain & Pal, 2017:792). A backdoor lets an attacker gain access to a system without having to provide login details. It also allows the attacker to perform malicious activity without leaving logs (tracking information) on the compromised system (King *et al.*, 2008:2).

3.2.3.7 Botnet attack

Botnets are systems that have been compromised, or hijacked, and are remotely controlled by attackers. These botnets are used for malicious intent and are sold by hijackers on the Internet. The botnets are then used by other actors to perform malicious activity, such as distributed denial of service (DDoS) attacks, to steal data, or send large amounts of spam (Jain & Pal, 2017:792). The word *botnet* comes from a combination of the words robot and network, which is exactly what a botnet is – a system that is controlled over the network. Botnets are controlled through a command and control channel that allows commands to be remotely executed to the bots (Gu *et al.*, 2008:139). There are generally two botnet structures, either centralised or a peer-to-peer (p2p) design. The bots in these structures receive commands from a botmaster using a push-and-pull method to execute tasks. The two structures are illustrated in Figure 3-6.

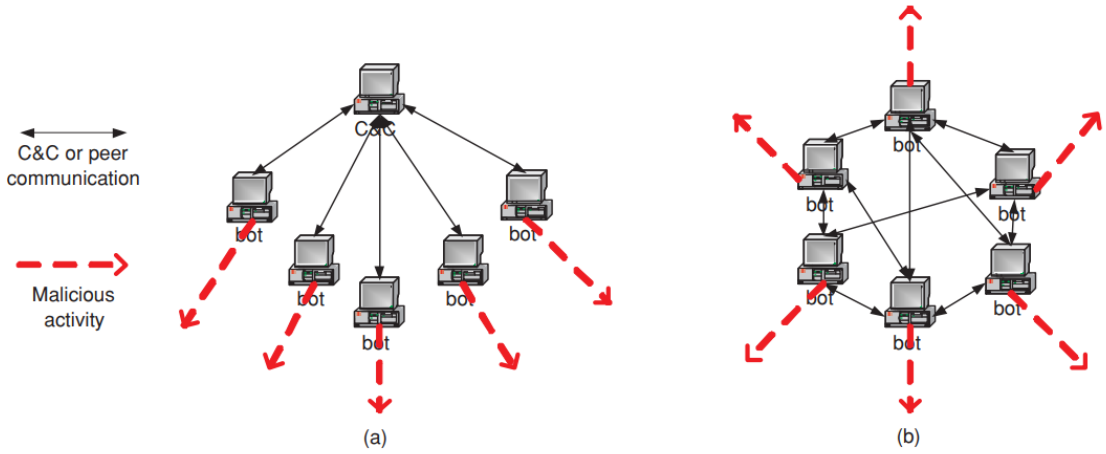


Figure 3-6: Two possible structures of a botnet: (a) centralised; (b) peer-to-peer (Gu *et al.*, 2008:142)

3.2.3.8 Social engineering

Social engineering is a term that hacker communities associate with utilising social interactions with users to gain sensitive information about a victim's information systems (Winkler & Dealy, 1995:1). Social engineers target the end users who have access to information systems (Krombholz *et al.*, 2015:114). However, attackers can also target high profile individuals using spear phishing attacks, which is an act that is also known as whaling. These social engineering attacks are specifically directed at the human element and not on that of the technical aspect of information systems (Krombholz *et al.*, 2015:117). The attacker's intention is that of manipulating the end users into divulging sensitive information. The attacker may also influence or persuade the victim to carry out malicious attacks.

The section that follows will discuss the different types of common social engineering attacks.

3.2.4 Types of social engineering attacks

With the growing digital landscape throughout the world, cyber-criminals are finding new and improved ways of exploiting vulnerabilities to gain access to computer systems. Users of information systems are often seen as the weakest link for cyber-attackers to gain access to information systems (Heartfield & Loukas, 2015:1).

The human element is the first point of attack. It is often the weakest element that cyber-criminals target in order to successfully exploit systems; this process is often achieved through a cyber-attack on humans known as a social engineering attack (Mouton *et al.*, 2016:187). Social engineering is the top-most preferred technique used by hackers and crackers to gain access to systems (Warwick, 2016).

In a paper compiled by Mouton *et al.* (2014a:4), they described social engineering as "*the science of using social interaction as a means to persuade an individual or an organisation to comply with a specific request from an attacker where either the social interaction, the persuasion, or the request involves a computer-related entity.*" Social engineering attacks are motivated by several goals, for financial gain, unauthorised access, or simply to cause service disruption. These attackers can either be single individuals or a group of individuals (Mouton *et al.*, 2016:188).

Social engineering attacks are presented in a variety of platforms, ranging from physical, social, and technical (Krombholz *et al.*, 2015:114). According to Conteh and Schmick (2016:32), the five most common social engineering attacks that are targeted at victims are phishing attacks, pretexting, baiting, quid pro quo, and tailgating. Krombholz *et al.* (2015:116) provide a taxonomy for social engineering attacks, which is illustrated in Figure 3-7. The taxonomy illustrates the

types, channels, and operators of social engineering. Additionally, the attack vectors of social engineering are also illustrated therein. Table 3-6 provides a summarised description of these attack vectors that were highlighted by Conteh and Schmick (2016:32), and in the taxonomy by Krombholz *et al.* (2015:116). These attack vectors are discussed in more detail in Section 3.2.4. It is important to note that some researchers do not consider dumpster diving and shoulder surfing as social engineering attacks, as they do not involve any form of social interaction with the victim (Ivaturi & Janczewski, 2011:3). For the purpose of this study, they will be considered as part of social engineering attacks as they involve the human element in some way.

Table 3-6: Combined common social engineering attack vectors from Conteh and Schmick (2016:32) and Krombholz *et al.* (2015:119)

Attack Type	Description
Phishing	Phishing attacks occur when users click on links that redirect them to legitimate looking but malicious websites that use fear tactics to scare users to divulge sensitive information.
Pretexting	An attack vector driven by creating a fake scenario in an attempt to compromise confidential information.
Baiting	This attack is similar to that of a phishing attack except that it lures victims into divulging sensitive information by promising them something if they provide the information.
Quid pro quo	This attack vector is commonly achieved through impersonation, where the victim is tricked into believing they are interacting with someone they are familiar with in order to divulge sensitive information.
Tailgating	This type of attack occurs when the attacker gains physical access to a restricted area by impersonating a trusted entity to the victims.
Dumpster diving	Dumpster diving, otherwise known as trashing, is a social engineering technique that is focused on an organisation's trash in order to possibly obtain sensitive information that is contained in documents that have been thrown away without being shredded.
Shoulder surfing	Shoulder surfing is a technique that is used to gather sensitive information by essentially looking over the victim's shoulder to obtain sensitive information.
Advanced persistent threat (APT)	Advanced persistent threats refer to long-term and mostly Internet-based espionage attacks, whereby an attacker intends to maintain access to the compromised system(s) for an extended period in order to mine sensitive data.
Reverse social engineering	Reverse engineering entices the victim into initiating the interaction, typically by fabricating a problem for the victim and presenting a viable solution.
Waterholing	It is a social engineering attack that requires a legitimate website (often used by the victim) to be compromised and used to obtain sensitive information from the target victim.

Figure 3-7 provides an overview of the social engineering taxonomy and its attack vectors.

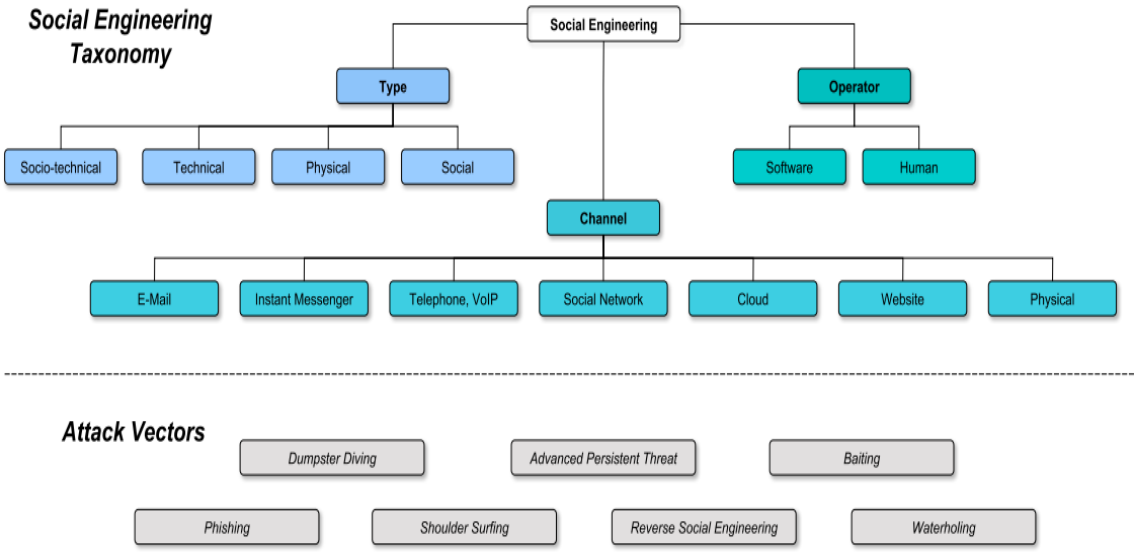


Figure 3-7: Overview of a social engineering taxonomy and its attack vectors Krombholz *et al.* (2015:116)

Figure 3-8 provides an adapted illustration of a combined view of the attack vectors for social engineering attacks as described by Conteh and Schmick (2016:32) and Krombholz *et al.* (2015:116).

Table 3-7 provides an outline of the relationship between the three different components of social engineering categories (channel, type, and operator) and the associated vectors for each category (phishing, shoulder surfing, dumpster diving, etc.). These vectors and categories are outlined in the taxonomy as in Figure 3-8.

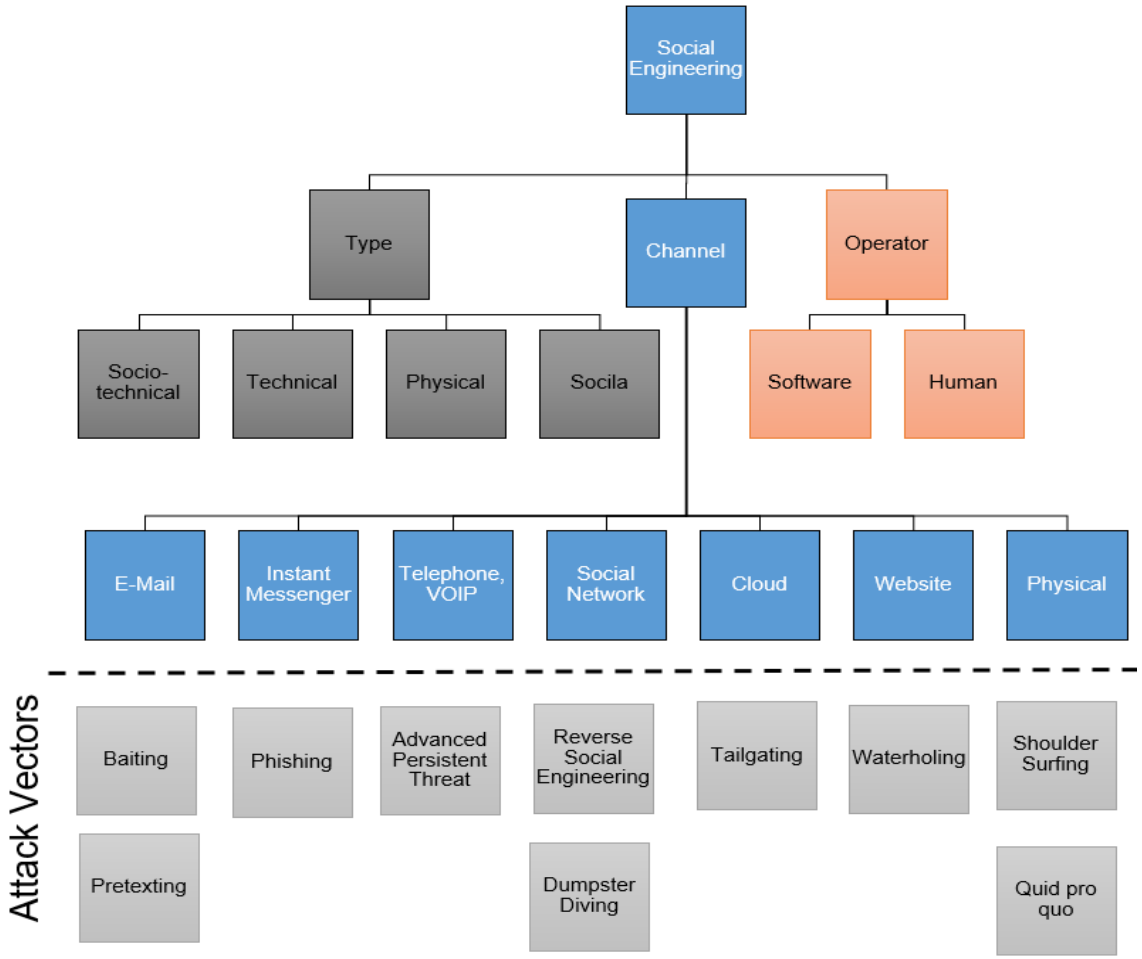


Figure 3-8: A combined view of the attack vectors in Table 3-6 and the social engineering taxonomy by Krombholz *et al.* (2015:116)

Table 3-7: Table adapted from the classification of social engineering attack vectors and social engineering categories by Krombholz *et al.* (2015:116)

		Phishing	Shoulder Surfing	Dumpster Diving	Reverse Social Engineering	Waterholing	Advanced Persistent Threat	Baiting	Pretexting	Tailgating	Quid pro quo
Channel	E-mail	✓			✓		✓		✓		
	Instant Messenger	✓			✓				✓		
	Telephone, VoIP	✓			✓				✓		✓
	Social Network	✓			✓						

		Phishing	Shoulder Surfing	Dumpster Diving	Reverse Social Engineering	Waterholing	Advanced Persistent Threat	Baiting	Pretexting	Tailgating	Quid pro quo
	Cloud	✓									
	Website	✓				✓	✓				
	Physical	✓	✓	✓	✓			✓		✓	
Operator	Human	✓	✓	✓	✓			✓	✓	✓	✓
	Software	✓		✓	✓	✓	✓				
Type	Physical		✓	✓				✓		✓	
	Technical					✓	✓				
	Social				✓						✓
	Socio-technical	✓			✓	✓	✓	✓	✓	✓	

In a study by Mitnick and Simon (2011:12), and as cited by Mouton *et al.* (2014b:2), they depict the stages a social engineering attack goes through, starting from the stage where information is gathered about the target, developing trust with the target, exploiting the trust that has been developed, and finally using this for malicious reasons or financial gain. This process is briefly illustrated in Figure 3-9.

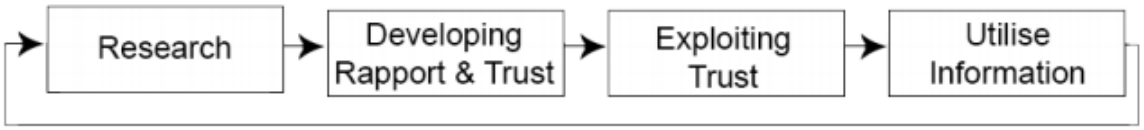


Figure 3-9: Mitnick's social engineering attack cycle (Mouton *et al.*, 2014b:2)

Mouton *et al.* (2014b:2) specify an ontological model for social engineering attacks. The model defines how social engineering attacks can employ direct or indirect communication, and is composed of a target (who is the victim), a social engineer (as the attacker), a goal (the objective of the attack), medium (for delivering the attack), and either one or more compliance principles and techniques. Each of these attack areas can be followed by multiple attack phases and target areas. This model is illustrated in Figure 3-10.

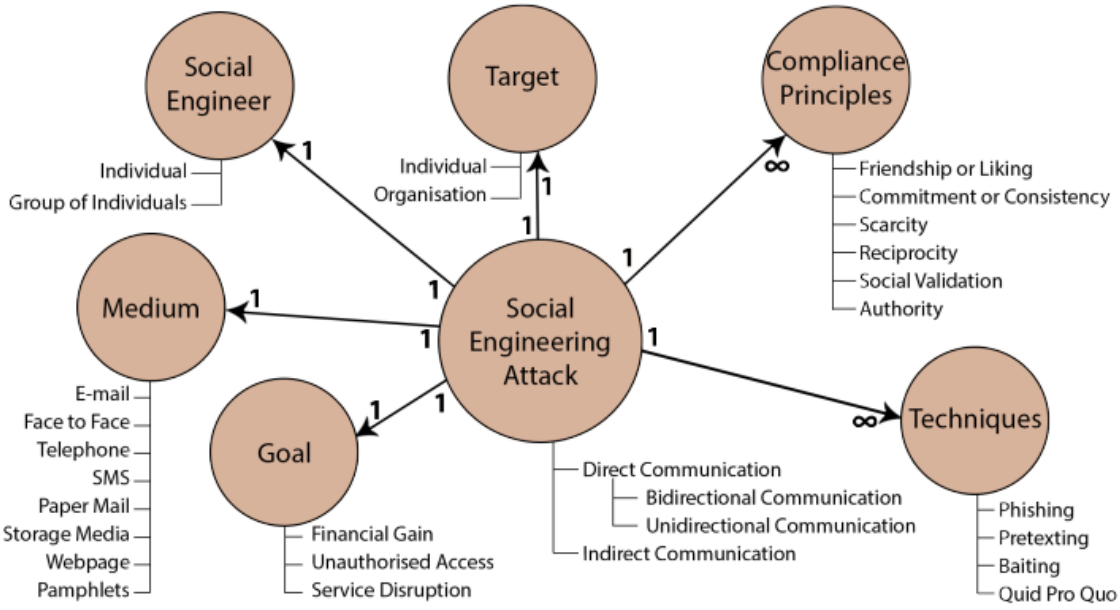


Figure 3-10: The ontological model of a social engineering attack (Mouton *et al.*, 2014b:2)

The success factor of social engineering attacks is driven primarily by the lack of understanding from the end-users on how to protect and prevent themselves from becoming victims of such attacks (Barrett, 2003:56). Educating end-users is the primary key to reducing the number of successful social engineering attacks (Wenjun *et al.*, 2017:3).

The next sections will discuss some of the most common forms of social engineering attacks, what they are, and how they are used to exploit the targeted victims.

3.2.4.1 Phishing

Phishing is a form of social engineering whereby sensitive information is fraudulently acquired by an attacker through impersonation as a trusted third party to the victim (Jagatic *et al.*, 2007:1). Phishing scams are growing more and more sophisticated and the statistics of people falling victim to these attacks is increasing. A report by Mimecast (2019), an email security company, indicated that 53% of South African companies have been affected by e-mail attacks. In the report, it was found that 94% of respondents experienced a phishing attack between 2018 and 2019, while 54% of the respondents experienced an increase in phishing attacks. An increase in spear-phishing attacks with malicious links was experienced by 45% of the respondents within the same period. Typical phishing scams may embed links to redirect users to suspicious sites that appear legitimate. A sense of urgency will typically be used to trick the user into divulging sensitive information (Conteh & Schmick, 2016:32).

It is important to note that there is a distinct difference between phishing and spear-phishing attacks. Spear-phishing attacks are fixated attacks that require initial data-mining to be carried out before the victims are attacked. This has proven to make spear-phishing attacks more successful because they are more personalised to the specific victims, whereas phishing attacks are more generalised. Spear-phishing is therefore considered to be a combination of technological approaches and social engineering (Krombholz *et al.*, 2015:115).

3.2.4.2 Pretexting

Pretexting is a social engineering attack where a fictional situation is created by an attacker in order to establish a trust with the victim, and then exploiting this trust to obtain sensitive information. Typically, the attacker will have some information about the target and may use this to obtain further information from the victim by confirming and requesting additional information (Conteh & Schmick, 2016:32). Pretexting is often more than simply lying to the victim; it involves a great deal of research and information gathering about the targeted victim (Ivaturi & Janczewski, 2011:4).

3.2.4.3 Baiting

Baiting is similar to phishing, except that the victim is lured through enticement strategies. This is typically achieved through promise of goods or rewards to entice the victims into divulging sensitive information (Conteh & Schmick, 2016:32). A typical example of a baiting attack is attackers leaving malware-infected USB (universal serial bus) storage media in a location that can easily be collected by unsuspecting victims. The USB is then plugged into a computer by the victim, which will allow the attacker to compromise the confidentiality, integrity, and availability of information (Krombholz *et al.*, 2015:115). The compromise typically occurs by exploiting the curiosity of people by enticing them to click on tempting files stored on the drives in order to execute the malicious payloads contained therein.

3.2.4.4 Quid pro quo

Similar to baiting, this attack works through impersonation. An attacker will typically impersonate someone who the victim is familiar with, such as an IT support personnel trying to assist with a computer-related problem. The attacker would use this as a platform to obtain sensitive information or transmit malicious programs onto the victim's computer (Conteh & Schmick, 2016:32).

3.2.4.5 Tailgating

This attack typically makes use of piggybacking techniques, where an attacker uses a victim's pre-authorised access to gain access to a restricted area. Typically, an attacker would impersonate a legitimate actor and would then be given access to an area by someone else within the organisation (Conteh & Schmick, 2016:32). The act of tailgating may be considered legal or illegal, based on the circumstances, but is generally associated with negative connotations. The attacker typically builds a character and fabricates a story around this character. The attacker will then use this fabricated character to persuade and convince a victim into giving them access to the restricted area. The attacker will have to be ready to answer questions once entered into the restricted area. To facilitate credibility of the fabricated story, the attacker can a) use company language in the story, and b) use knowledge obtained about personnel who work for the company (Ivaturi & Janczewski, 2011:5).

3.2.4.6 Dumpster diving

Although this is not rated as one of the most common social engineering attacks, it is worth including in the descriptions as it is less difficult to execute than other forms of social engineering attacks. Dumpster diving, otherwise known as trashing, is a social engineering technique that is focused on obtaining information from an organisation's trash (Luo *et al.*, 2011:5). The attacker searches through the trash in order to possibly obtain sensitive information that is contained in documents that have been thrown away without being correctly shredded (Krombholz *et al.*, 2015:114). These documents may contain information such as employees' personal data, manuals, memos, or even printouts of information such as credentials or diagrams of the organisation's network infrastructure (Granger, 2001:4).

3.2.4.7 Shoulder surfing

Shoulder surfing is a technique that is used to gather sensitive information by essentially looking over the victim's shoulder to obtain sensitive information such as usernames and passwords (Long, 2011). A simple example that many people are familiar with would be a malicious person trying to peer over your shoulder at an auto teller machine (ATM) to possibly try and obtain your banking pin or other banking details.

3.2.4.8 Advance persistent threat (APT)

Advanced persistent threats refer to long-term, and mostly Internet-based espionage attacks, where an attacker intends to maintain access to the compromised system for an extended period

in order to mine sensitive data (Krombholz *et al.*, 2015:117). APTs occur over three stages (Anonymous, 2019):

1. Network infiltration, where the systems are compromised either through vulnerabilities or through human interaction;

2. Expansion, occurs when the attacker moves through the network environment, compromising more systems; and

3. Extraction, which is the stage when the sensitive information is extracted from the network, typically under the cover of white noise, which occurs when the attacker launches a DDoS attack to distract the IT security team while moving the stolen data out of the network.

3.2.4.9 Reverse social engineering

This attack is the reverse of the approach a typical social engineering attack would take. Similar to quid pro quo, reverse social engineering does the opposite. Instead of initiating the interaction with the target victim, reverse engineering entices the victim into initiating the interaction, typically by fabricating a problem for the victim and presenting a viable solution (Breda *et al.*, 2017:4). These type of attacks involve three major parts: sabotage, advertising, and assisting (Krombholz *et al.*, 2015:115). *Sabotage* occurs when the attacker causes a disruption to the IT systems of the victim. *Advertising* occurs when the attacker advertises to the victim that they can resolve their issue legitimately, which leads the victim into allowing the attacker, who appears legitimate, to assist them. The attacker pretends to *assist* the victim, but is actually stealing sensitive information in the process.

3.2.4.10 Watering hole

Considered to be one of the most advanced social engineering attack vectors due to the technical requirements needed to execute it, waterholing is a social engineering attack that requires a legitimate website (often used by the victim) to be compromised which is subsequently used to obtain sensitive information from the target victim (Breda *et al.*, 2017:5). It is described as an attack where a website that is of interest to the victim is compromised, then the attacker waits at the *waterhole* (the compromised website) for the victim to click, download or enter their confidential information (Krombholz *et al.*, 2015:117).

3.2.5 Raising cyber-security awareness

In this portion of the study, some of the techniques used to deliver information security awareness to users about social engineering attacks are discussed.

Users of information systems are often unaware of the security risks they are exposed to when using these technologies (Shaw *et al.*, 2009:93). Educating users about the cyber risks when using technology can be achieved by improving their information security awareness. Abawajy (2014:237) defines this awareness as the level of comprehension users have about the importance of information security best practices. Shaw *et al.* (2009:92) provide a clearer definition of cyber security awareness by stating that it is "*the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organisation's data and networks.*" Awareness has three levels, which are mainly perception, comprehension, and projection. Shaw *et al.* (2009:92) identify three barriers to information security awareness, which are: 1) general security awareness, 2) employee computer skills, and 3) budget of the organisation.

There are technology-based tools such as firewalls, spam filters, and web filters that are available to protect users from certain social engineering (SE) attacks. It is important that users do not become too reliant on these tools and should also seek to increase their awareness through phishing training as well as other approaches to raise awareness of these social engineering attacks (Jansson & von Solms, 2013:585). Hendrix *et al.* (2016:55) examine a number of papers that evaluate research that has been conducted on cyber-security training games. In the study, 28 papers were evaluated. The papers indicated that the most popular types of games were three-dimensional (3D) and simulation games, followed by mobile applications. Table 3-8 provides a summary of literature available regarding the different games to raise security awareness.

Table 3-8: Results of an evaluation of different research papers on cyber-security training games (Hendrix *et al.*, 2016:55)

Game name	Game type	Methodology	Results
TiER I	Interactive role-play	EEG and eye tracking	Unclear
Anti-Phishing Phil	Mobile application training safety of link URLs	Think aloud, pre-test & post-test experimental vs. control, SUS usability questionnaire	Positive impact on learning, awareness, and phishing susceptibility
Security games by Next Generation Security (NGSEC)	Web-based	Comparing on-task performance	Significant improvement in game group
CyberCIEGE	3D virtual world (rims style)	Unclear Experiment & self-assessment Theoretical review of cognitive principles (1191)	Sufficiently flexible to illustrate a wide range of topics and positive early indication Positive Unclear, but there is a need to create a science of games

Game name	Game type	Methodology	Results
			Conclusions about software development
PicoCTF	Web-based	Survey	Positive educational experience according to students & instructors
Control-Alt-Hack, [dOx3d!],	Puzzle card & board games	Puzzles used as assessment in class in 2 groups (intervention vs. control) Playing together Survey of 22 educators teaching 450 students	Initial feedback positive, but more formal evaluation needed Game is effective model for dissemination
Baltic Cyber Shield (BCS) international cyber defence exercise	Large training exercise with group of virtual attackers and defenders	Lessons learnt (informal)	A number of recommendations for IT infrastructure management
No specific games mentioned	Unclear	Review of initiatives	Initiatives need more synergy, no conclusions about games
The Internet	Unclear	Literature review	A review of elements a security network game should have
Internet Hero	Puzzle mini-games	Experiment with children	The children liked the games
Security awareness program	Unspecified	Experiment with pre-test & post-test	No significant increase in awareness
CyberNEXS	Network Simulation	None	Overview of game design
None (review paper)	Various	Literature review	More tools need to be developed
A series of interactive visualisations	Interactive visualisation	Case study	Account of positive experience of using interactive visualization
Multimedia and Interactive Courseware Synthesizer	Website with interactive animations	None	None

Table 3-9 by Hendrix *et al.* (2016:55) lists a number of games that are mainly targeted at children, teenagers, students, and corporate individuals. The main difference between Table 3-8 and Table

3-9 is that Table 3-8 summarises the cyber security educational games that were evaluated in other research papers. Table 3-9 is a summary of games for cyber security education that are available online.

Table 3-9: Products available to raise cyber-security awareness (Hendrix *et al.*, 2016:57)

Game Name	Game Type	Topic / learning outcome	Target audience
CyberCIEGE	3D virtual world (rims style)	Information security for enterprise	Science curriculum students
CyberSecure Contingency Planning	2D point & click turn-based scenarios	Contingency planning to prevent data loss at health practices	Health practice decision-makers
CyberSecure Your Health Practice	2D point & click turn-based scenarios	Contingency planning to prevent data breaches at health practices	Health practice decision-makers
OnGuard	2D point & click turn-based scenarios	Online security (viruses and malware as well as social networks)	Teenagers / Children
Budd:e	2D point & click turn-based scenarios	Staying safe online (viruses and malware as well as social networks)	Children
NSteens	Mini-games: 2D point & click turn- based scenarios and puzzle games	Staying safe online (viruses and malware as well as social networks)	Teenagers
Carnegie Cadets	Various 2D mini- games	Staying safe online (viruses and malware as well as social networks)	Children
McGruff	2D point & Click	Staying safe online (viruses and malware as well as social networks)	Children
FBI Cyber Game	Puzzle games	The FBI, it's history and staying safe online	Children
PBS Cybersecurity Lab	2D puzzles with extensive narrative cuts-scenes	Staying safe online, spotting scams and defending against cyber attacks	Children
The Cyber Security Challenge	National competition	Over 20 different competitions on various topics	School and university students
The Cyber Security Challenge UK	National competition (physical role-Play)	Over 20 different competitions on various topics	School and university students

Game Name	Game Type	Topic / learning outcome	Target audience
Game of Threats	Partially digital via tablet controller, but controlled by facilitators	breach (companies being hacked into and losing data / data being compromised)	Companies
High School Cyber Security Game - global cyberlympics	Global competitions, exercises scored by human facilitators	Forensics, and computer network defence	High School students
CyberProtect	2D simulation	Fundamentals of Cyber Security and Information Assurance	Students and security professionals
Cyphinx	Virtual world with puzzles	Various	Students and young adults

Over and above the technological approaches to raising cyber security awareness, organisations also need to enforce well-defined policies and procedures to help defend against social engineering attacks. Organisations often neglect the importance of educating their employees around the possible cyber-security threats they may be exposed to when using information systems. This issue of neglect has seen organisations suffering compromise of sensitive information as a result of a lack of awareness of the warning signs of social engineering attacks (Jansson & Von Solms, 2011:24). Abawajy (2014:239) makes mention of six delivery methods to raise information security awareness, which are summarised in Table 3-10.

Table 3-10: Cyber security awareness delivery methods and their example training material (Abawajy, 2014:239)

Delivery method	Description	Training material assessed in the study
Conventional delivery	Conventional methods used to deliver information security awareness, which include electronic resources and paper-based resource.	A shorted online article explaining phishing and its preventative measures (http://websearch.about.com/od/dailyweb searchtips/qt/dnt0810.htm).
Instructor-led delivery	Delivery methods that typically occur in the form of formal presentation seminars in a classroom fashion that is facilitated by an expert in the industry.	N/A

Online delivery	Online delivery methods would include channels such as e-mail broadcasting, blogs, repositories, animation, and multimedia.	N/A
Game-based delivery	Delivery methods that combine graphics, play, and training concepts to create compelling training experiences.	Master of Security (http://www.kongregate.com/games/gmentat/master-of-security), AntiPhishing Phil (http://wombatsecurity.com/antiphishing_phil/index.html) and CyberCIEGE (Cone *et al.*, 2007).
Video-based delivery	Online video is a medium that provides visual and audio learning for participants.	'How to Avoid Phishing' (http://www.5min.com/ Video/How-to-Avoid-Phishing-12254) video.
Simulation-based delivery	A simulation training where user awareness is tested through a phishing campaign and is followed by awareness training.	N/A

The sections that follow provide examples of some of the innovations created to raise awareness around social engineering (discussed in Section 3.2.5.1), cyber-security (discussed in Section 3.2.5.2), and the game-based delivery methods available to raise awareness on both social engineering and cyber-security (discussed in Section 3.2.5.3).

3.2.5.1 Social engineering awareness delivery methods

Bullée *et al.* (2015:103) present a study that explores the extent to which an intervention can reduce the effects of social engineering in an office setting. The intervention consisted of the following three artefacts:

1. A leaflet which indicated the dangers of social engineering how they should be identified and remediated once identified (refer to Figure 3-11);

2. A blue key chain that depicted the university's logo and advisory text on the other side (refer to Figure 3-12); and

3. A poster providing awareness on avoiding sharing secretive information such as passwords, keys, or personal identification numbers (PIN) (refer to Figure 3-13).

Figure 3-11 depicts the leaflet that was presented to the participants. Figure 3-12 illustrates the key chain that was used as part of the illustration, as a way to provide subtle reminders of what not to do.

Memo September 4, 2013

Do you share your PIN, key or password?

Your PIN, key & password, belong to you, are yours only and not meant to share. Sharing this is dangerous and therefore by many organisations forbidden, this also is forbidden by the University of Twente. Once this information are shared it is out of your control and could cause harmful situations with catastrophic consequences to both you and the organisation. Such as fraud or information theft as can be seen in the video[1].

You could also be victim of an information thief. Most dangerous part of these attacks is that you would not notice when you are under attack. Requests that look legitimately and could be explained rationally are hard to distinguish from unjustly requests. On the occasion that someone claims to be from the IT department and asks for you IP-address, this all sounds all justifiable. How to be sure that the person you are talking to is really who he claims to be? Challenge the requester with specific questions that validate the identity.

Information thieves more often exploit end users of a system to bypass security mechanisms. Technical security mechanisms grow stronger and become harder to abuse. Most employees are no expert in the area of computer systems, and this is known by thieves. This makes every employee interesting for attackers and thus important in the security chain. Especially since we are helpful by nature.

Attackers use identities from someone else to trick targets into revealing sensitive information. Effective ways to do this is to pick someone who has authority, for example a manager, a lawyer or a doctor. Experiments show that a stranger was able to collect 60% of the username and password combinations within a medium sized company, just by asking employees for it.

Information thieves abuse employees to get access to computer networks. By impersonating people with authority, thieves are successful in obtaining user credentials and other useful information. This is all done, without the victim noticing it. If someone asks for information related to the computer system, validate their identity before you give any information. And never ever share your password, key or PIN with anyone. Help protecting yourself against information thieves with the special awareness key-chain. This key-chain is available for you at your secretary.

Do Not...	Do...
• give your credentials away	• challenge the requester
• say Yes to often	• be critical and suspicious
• share valuable information via a phone call	• ask for name + phone number and redial

[1] http://www.youtube.com/watch?v=IhXfCzCjHWA

UNIVERSITY OF TWENTE.

Figure 3-11: Memo used in the intervention (Bullée *et al.*, 2015:104)

Figure 3-12: Key chain (Bullée *et al.*, 2015:105)

Figure 3-13 illustrates the poster that was created as part of the intervention.

Figure 3-13: Poster used in the intervention (Bullée *et al.*, 2015:105)

The results of the study indicated that the interventions used to raise awareness around the dangers of social engineering attacks did have a positive effect on deterring successful attacks. This was confirmed through a social engineering attack that was performed on two separate groups of employees within an office environment. The first group of employees were subjected to a social engineering attack without any prior intervention and the number of employees who fell victim to attack was recorded. The interventions depicted in Figures 3-11 to 3-13 were presented to the second group of employees after which a social engineering attack was performed. The results of the attack were also noted. The results indicated that the employees who were presented with the interventions showed a 25% reduction in susceptibility of falling victim to the social engineering attacks (Bullée *et al.*, 2015:97).

3.2.5.2 PowerPoint slideshow to raise cyber-security awareness

In another study conducted by Schilder *et al.* (2016:286), titled '*The effectiveness of an intervention to promote awareness and reduce online risk behaviour in early adolescence'*, they created an intervention that was composed of a PowerPoint slideshow presentation containing

simple wordings and graphics that illustrate the possible dangers of using computers and the Internet. The slides covered five different risk areas the users may be exposed to. The risk areas were textual contact, audio-visual contact, social network services, online games and contests, and the fifth being offline meetings with people met online. An example of some of the slides is illustrated in Figure 3-14 below.

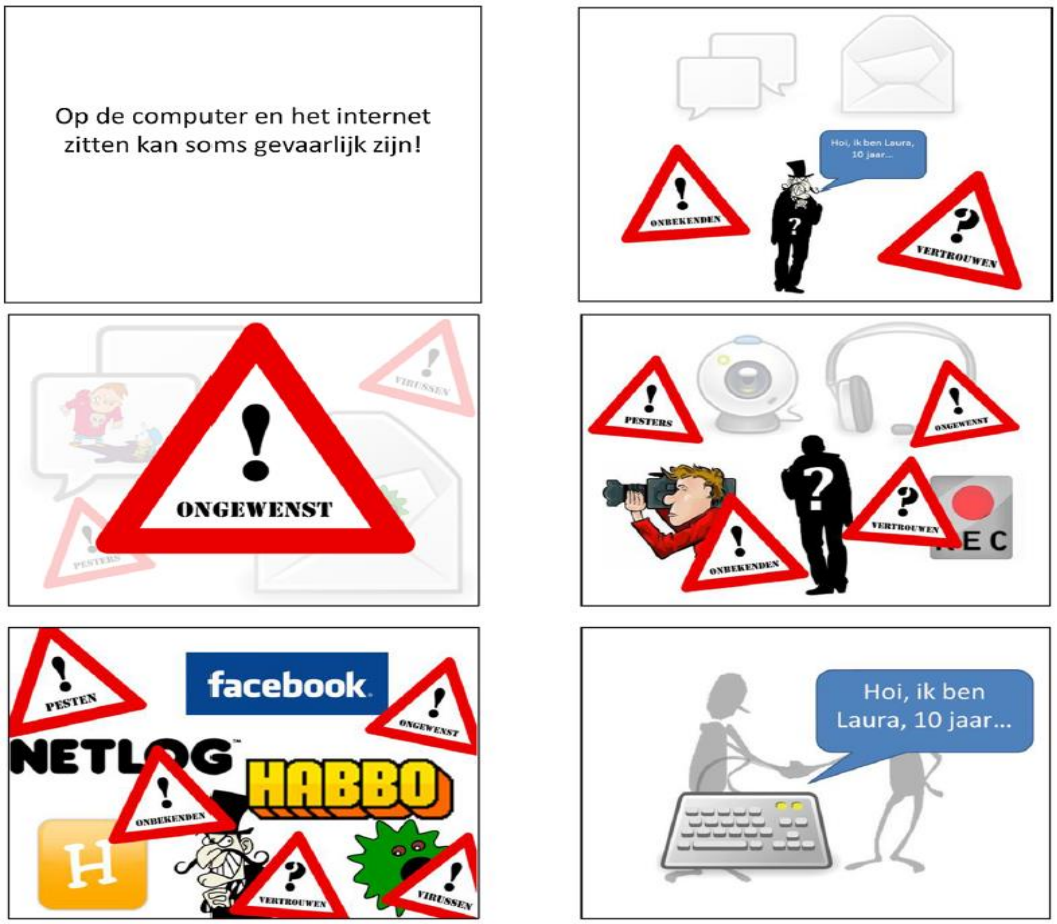


Figure 3-14: Artefact (PowerPoint slideshow) used to raise cyber awareness during early adolescence (Schilder *et al.*, 2016:296)

The results of the study indicated that risk awareness was significantly increased in the target group and that the number of reported cases of online risk behaviour had decreased after exposure to the intervention. This was confirmed by presenting a Likert scale questionnaire to the participants (who were children). The participants were presented with an artefact and the questionnaire again. It was statistically determined that the children's awareness, based on the questionnaire results, had increased (Schilder *et al.*, 2016:293). There were some limitations in the study that were noted such as the limited time frame the questionnaires were delivered to the participants in order to test the long term effects of the interventions, as well as the limitation that

the questionnaires used were designed to cater specifically for the study needs but were not questionnaires that were repeatedly tested in several studies to ensure they yield similar results. Additionally, issues such as cultural differences in the participants should also be considered in future studies.

3.2.5.3 Game-based delivery methods to raise cyber-security awareness

This section briefly describes game-based artefacts that were created to raise awareness regarding cyber-security.

3.2.5.3.1 CyberCIEGE

Other delivery methods to raise cyber-awareness include game-based delivery such as the CyberCIEGE video game, which was developed by the Naval Postgraduate School in the United States (Cone *et al.*, 2007:64). The 3D video game provides support in education and training around computer and network security. The game is composed of the following elements: "*a unique simulation engine, a domain-specific scenario definition language, a scenario development tool, and a video-enhanced encyclopaedia*" (Cone *et al.*, 2006:433). Development of CyberCIEGE occurred in an iterative manner. The artefact was made of the components as illustrated in Figure 3-15.

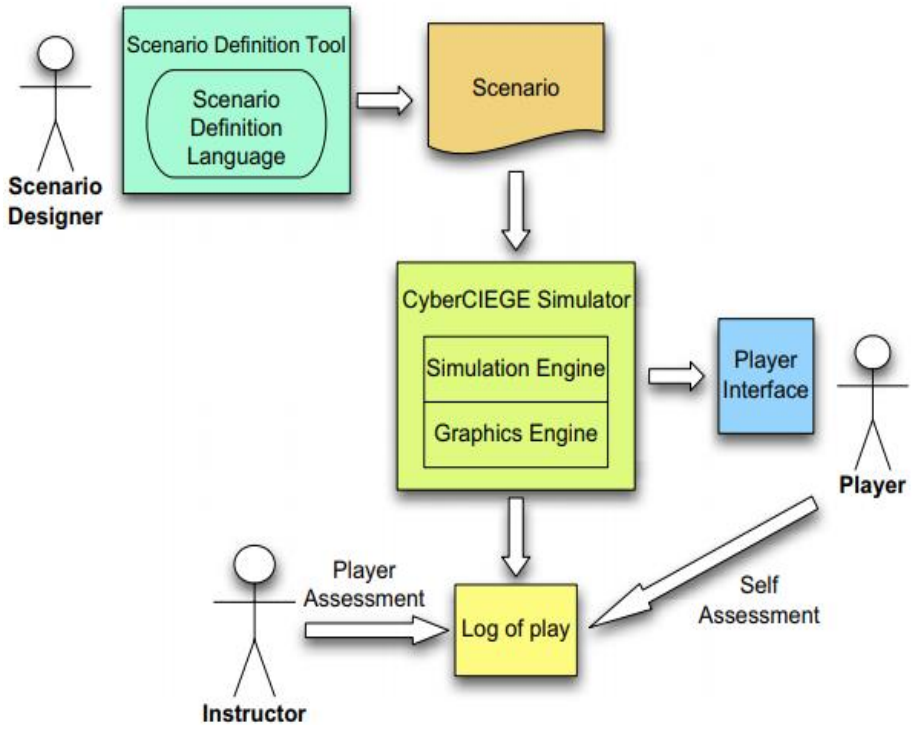


Figure 3-15: The CyberCIEGE components (Cone *et al.*, 2007:65)

CyberCIEGE required users to complete multiple phases. For a player to move on to a subsequent phase, the game would check whether prior phases had been completed. The game responded using active triggers and would change states according to elapsed time, goal achievement, etc. The triggers involved brief movies, changes in user goals, user feedback, and pop-up messages. Figure 3-16 provides an illustrative example of what the 3D game looked like, with an example of a trigger in the form of a pop-up message.

Figure 3-16: CyberCIEGE illustration of an in-game pop-up (trigger) message (Cone *et al.*, 2007:67)

The effectiveness of CyberCIEGE had not been assessed, although feedback from the participants who were testing the artefact was noted to be positive. CyberCIEGE has undergone multiple changes and improvements noted in other studies and has been used by many organisations as a training tool.

A demo version of CyberCIEGE demo can be accessed at the unified resource link (URL): https://my.nps.edu/web/c3o/downloads

3.2.5.3.2 Game of Threats

Game of Threats is a game-based tool that was designed by PricewaterhouseCoopers (PWC) to mimic a cyber-attack that is happening on an organisation (Kirton, 2017:43). It engages participants in a gamified scenario where the participants are required to actively participate in the simulation rather than just engaging with some artefact.

Game of Threats divides the participants involved in the simulation into two teams, the attackers and defenders in the company. Each of the team members is given an iPad controller, which is used to make decisions throughout the gameplay. The moderators provide a detailed summary of each game, reviewing the strategy used by both teams (PWC, 2015).

There is no unified resource link (URL) available to play or download this game, as it was not publically released by the developer.

3.2.5.3.3 CyberProtect

CyberProtect provides students and cyber-security professionals with a platform to learn about the fundamental aspects of cyber-security and information assurance (Hendrix *et al.*, 2016:57). It is "*a web-based, interactive computer network defensive exercise with a video game look and feel*. *It is intended to familiarise players with information assurance security terminology, concepts, and policy. Players learn about defensive security tools, which must be judiciously deployed on a simulated network*" (Carney & Department of Defense, 2010). A graphic representation of the in-game interface is provided in Figure 3-18. Figure 3-17 provides a representation of the in-game menu that the user is initially presented with when starting the game.

Figure 3-17: CyberProtect in-game menu (screenshots taken from Carney and Department of Defense (2010))

Figure 3-18: CyberProtect in-game view (screenshots taken from Carney and Department of Defense (2010))

CyberProtect can be accessed at unified resource link (URL): https://iatraining.disa.mil/eta/cyber-protect/launchcontent.html

3.2.5.3.4 Anti-Phishing Phil

Anti-Phishing Phil is an online game that aims to teach people on the awareness of phishing attacks and avoid being victims of these attacks (Sheng *et al.*, 2007:1). It teaches people to identify phishing URLs, where to look for suspicious cues on a web browser, as well as how to use search engines to find legitimate sites. There are four types of learning science theory methodologies for game development, which are that the game must be goal-oriented, challenging, contextual, and interactive. Figure 3-19 presents the Anti-Phishing Phil start menu to play the game.

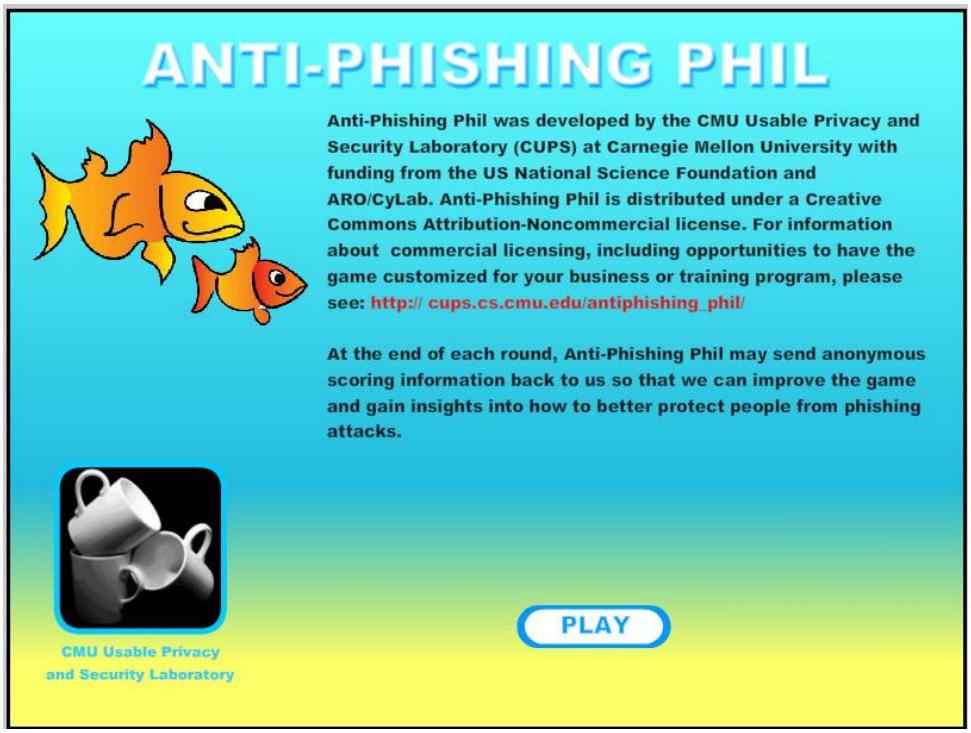


Figure 3-19: Anti-Phishing Phil start menu (screenshot taken from Sheng *et al.* (2008))

Figure 3-20 depicts the pre-game instructions menu that explains to the player how the game should be played.

Figure 3-20: Anti-Phishing Phil pre-game instructions menu (screenshot taken from Sheng *et al.* (2008))

Figure 3-21 depicts the flow of the game: the pre-round lesson that teaches the player about the concept important for the round, the in-game view when playing the game, and the scoreboard that allows the player to reflect on their progress and either go to the next round or retry the level.

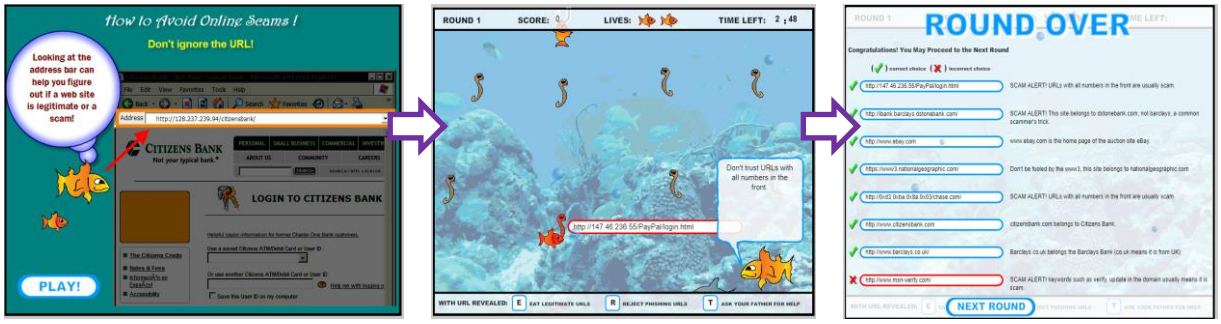


Figure 3-21: Anti-Phishing Phil game flow: pre-round lesson, in-game play view, and end of round scoreboard (screenshot taken from Sheng *et al.* (2008))

Anti-Phishing Phil can be accessed at the unified resource link (URL): https://www.ucl.ac.uk/cert/antiphishing/

3.2.5.3.5 Master of security

Master of security is a game that aims to teach users about the basic concepts of cyber security. The player needs to protect his software from harmful threats, which include threats such as adware, spyware, viruses, etc., by building security shields on the game desktop. This is achieved by changing the movement and directions of the invaders by redirecting them through a longer route, which provides the player's shields time to destroy the threats. Figure 3-22 depicts the Master of security instruction menu.

Figure 3-23 depicts the flow of the game, which starts with the menu that allows the user to set specific parameters about the game. The gameplay screen is depicted, as well as the scoreboard, which allows the player to reflect on the game play and to restart the game, save their score, or return to the main menu.

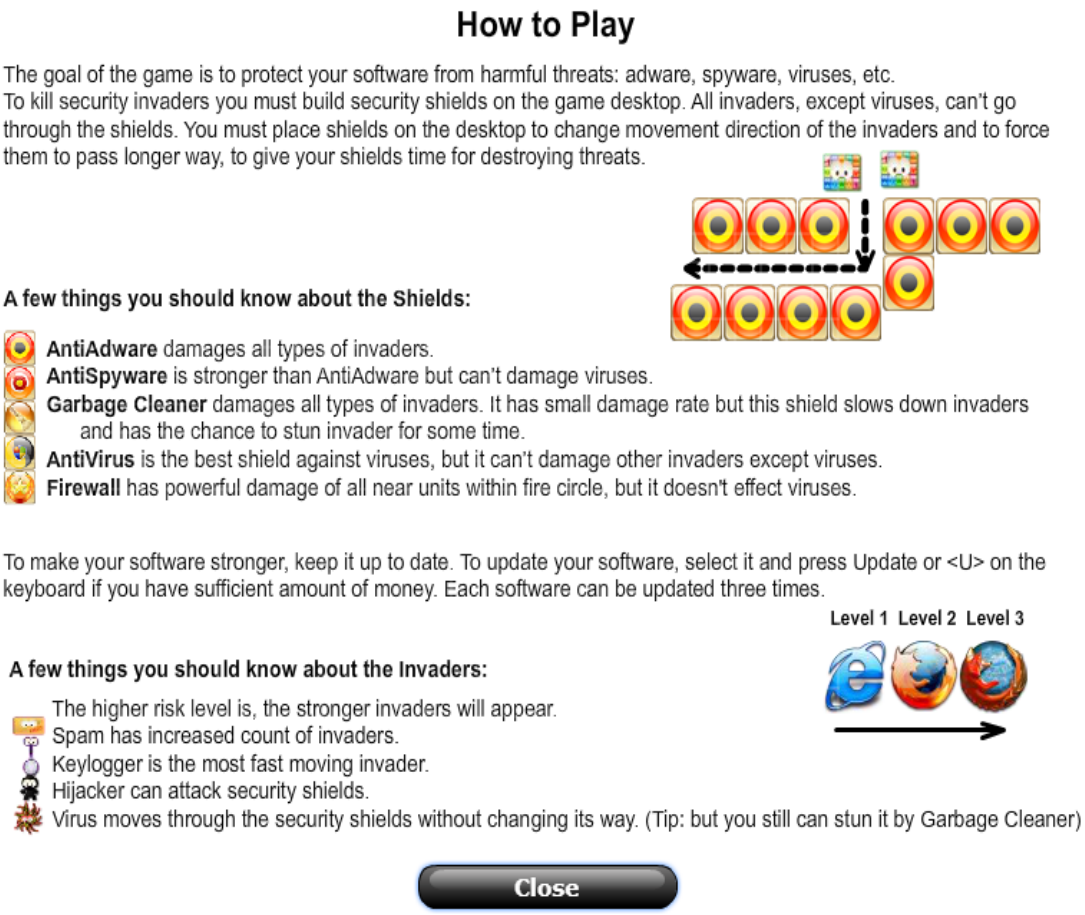


Figure 3-22: Master of security in-game instructions menu (screenshot taken from Anonymous (2008))

Figure 3-23: Master of security game flow: main menu, in-game play view, and end of game scoreboard/menu (screenshot taken from Anonymous (2008))

Master of Security can be accessed at the unified resource link (URL): https://www.kongregate.com/games/gmentat/master-of-security

The next section will conclude on the observations noted from this chapter of the study.

3.3 Conclusion

In this section of the study, a variety of cyber security issues, as well as the different attack vectors and motivations behind these cyber-attacks, were discussed. It is clear from these issues discussed that cyber-attackers are improving their methods for compromising systems and that the human element is an aspect that requires significant attention as it is often the weakest point in an organisation's security posture (Shaw *et al.*, 2009:92). The human element is exploited through an attack known as a social engineering attack.

It was further noted that social engineering as a cyber-crime has a variety of vectors that can be used by an attacker to compromise the human element. This would allow the attacker to gain sensitive information or even compromise a system. In order to overcome these issues around social engineering attacks, education pertaining to social engineering attacks is necessary. Education is the primary defence mechanism to strengthen the vulnerabilities within the human element (Schlienger & Teufel, 2003). Awareness and training programmes will lead users to become aware, stay aware, and be aware of cyber security risks.

From a perspective of educating the weakness in the human element, a variety of artefacts that could be used to improve or increase an end-user's awareness to social engineering attacks were assessed. The effectiveness of these artefacts was not assessed specifically in this study.

Based on the literature conducted in this chapter, a suitable method to raise awareness for social engineering is game-based delivery. The design process of a game-based artefact will tie into the processes defined in Chapter 2 of this study. In the next chapter, the process of designing a game-based prototype that can be used to raise cyber-awareness will be discussed. Design science research (DSR) is the preferred research approach for developing the game-based artefact.

CHAPTER 4: THE DSR APPROACH FOLLOWED IN THIS STUDY

4.1 Introduction

The primary objective of this study is to design and develop an artefact that can be used to raise awareness about social engineering attacks among administrative staff in medium to large organisations. This chapter will support this primary objective by describing the design science research approach that is followed in designing and developing the artefact. The artefact development undergoes three stages: (1) a pre-design stage, where a conceptual artefact is developed; (2) a mid-design stage, where a prototype is developed; and (3) a post-design stage, where the artefact is evaluated to determine whether it addresses the primary objective of the study.

For this particular study, the design science research methodology (DSRM) process model by Peffers *et al.* (2007:54) is used to guide the research document (see Section 2.4.1.2 for DSRM process model discussion). The research objectives, which are structured according to the DSRM process model, are discussed in Section 2.5.1.1. The design science research cycles by Hevner (2007:2) are used to guide the process of designing, developing, and evaluating the artefact (see Section 2.4.1.3). The artefact will be created through a cyclical (also referred to as iterative) approach until a final product is reached. The artefact design, development, and evaluation process is briefly discussed in Section 2.5.1.2.

In this chapter, the researcher will discuss the approach to applying the cycles of the DSR process as defined by Hevner (2007:2). It is important to note that the three-cycle view of design science research (as illustrated in Figure 4-1) embodies a number of activities relevant to each cycle. The relevance cycle initiates the DSR process within an application context that provides the research requirements as inputs, as well as the acceptance criteria to evaluate the research results. The rigor cycle uses prior knowledge to the research to ensure design innovation. It also produces additions to the knowledge base. The central design cycle is an iteration (iteration and circuit used interchangeably in this study) of the building and evaluation of the artefact design and applicable processes thereof.

The DSR cycles by Hevner (2007:2) complement the approach that was followed by Mckenney and van den Akker (2005:49) in their evaluation of the CASCADE-SEA program (discussed in Section 2.4.4). Additionally, the process is suitable in that it involves the participants for whom the artefact will be designed. The involvement of the participants will guide the design of the artefact, from the inception of the conceptual design, to the prototype. The Mckenney and van den Akker (2005:49) diagram (Figure 4-2) will be adopted as a reporting tool for this study.

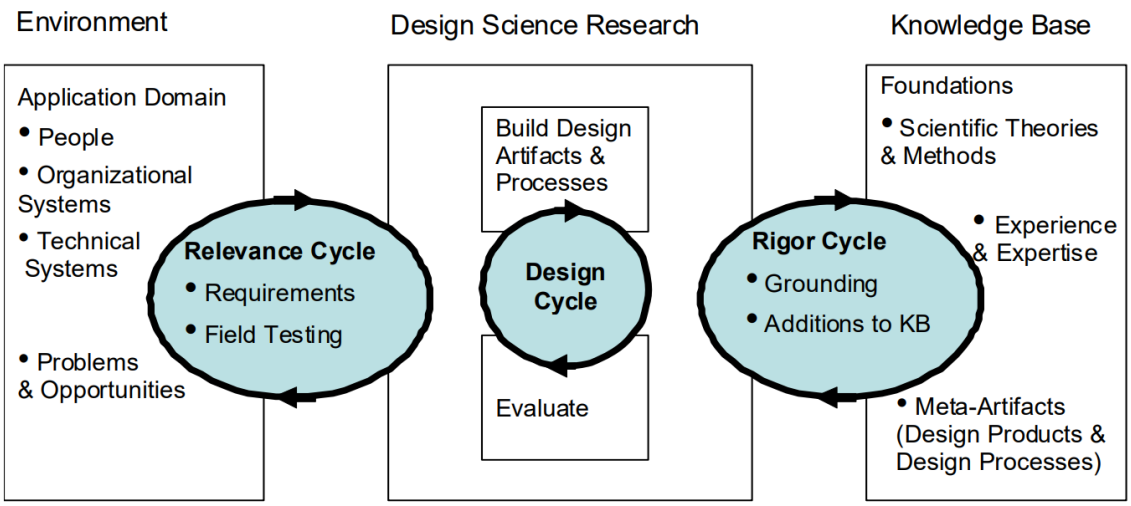


Figure 4-1: The design science research cycles (Hevner, 2007:2)

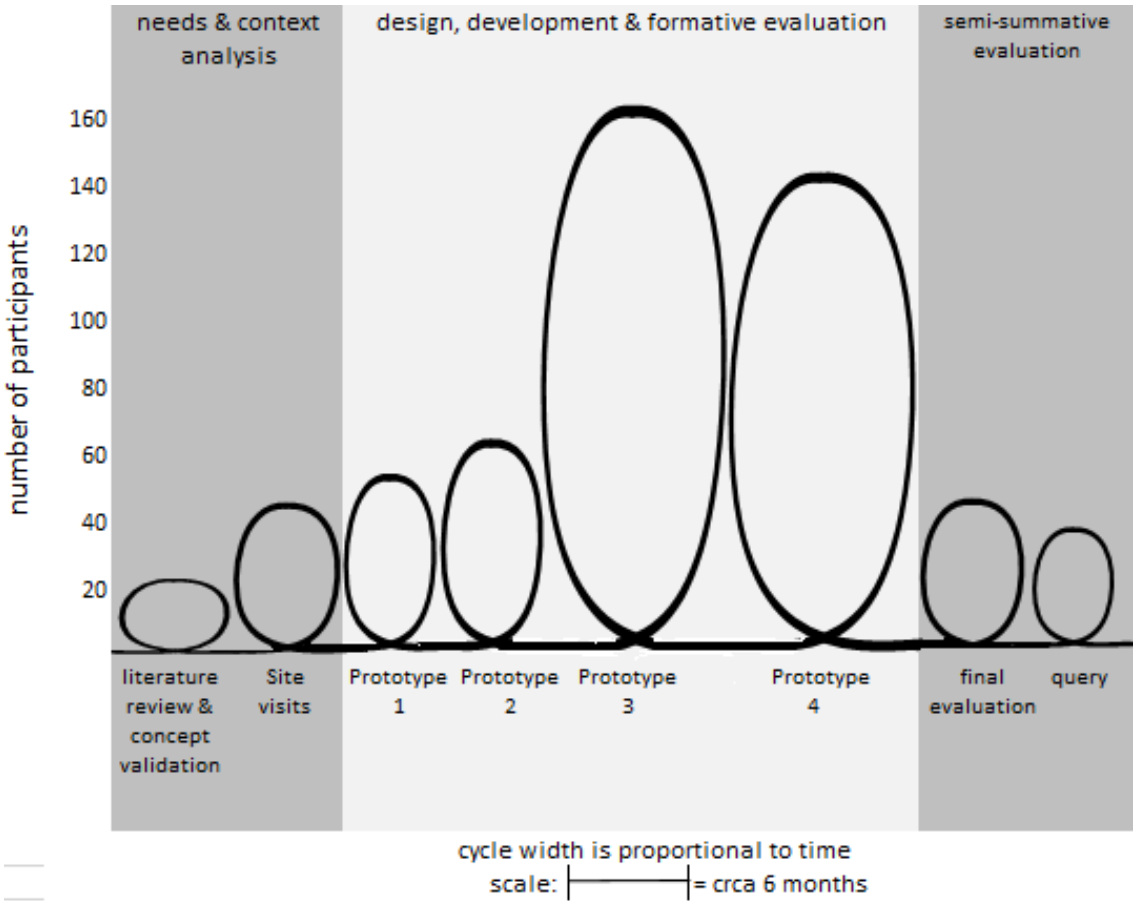


Figure 4-2: Cyclical approach to the three phases followed by Mckenney and van den Akker (2005:49)

In this study, a game-based delivery is the vehicle for presenting the social engineering information. The type of artefact was chosen based on the literature as well as the development skills that the researcher possessed. The focus of this study is on the development of an artefact that can be used to raise awareness. This type of game that addresses a serious education matter is sometimes referred to as a serious game. Digital games-based learning, or otherwise known as serious games, are games that instigate learning through a process of engagement (Brom *et al.*, 2014:69). Serious games put a strong emphasis on learning rather than on entertainment. As the focus of this study is on the development of the artefact following a DSR approach and not yet on the emancipation of its users, it will not be referred to as a serious game, but only as a game-based artefact. Based on the methodology selected, the design of the artefact will be driven by the target user group.

The first workshop that will be held with the target user group will provide input and direction to the initial conceptual design of the artefact. The information collected for the conceptual design will determine the key elements of the game, such as the in-game resources, the storyline, elements of interest to the users, colour schemes, characters, etc. Frequent workshops with the target user group will be held to ensure the design is evaluated and remains relevant. Expert opinion (from academia and industry) will be sought within the fields of design science research, cyber-security, game design, and user experience design to ensure an acceptable level of quality is built into the design prototypes. Provision is made for a conceptual design and two full prototypes of the game. The completion of the second prototype will be evaluated as a summative evaluation and testing using a set of criteria as described by Petri and von Wangenheim (2016:995), which was the four-level model discussed in Section 2.4.2.

4.2 Relevance cycle

For the relevance cycle, the researcher needs to gather the requirements necessary to build the artefact, and the key criteria that will be used to evaluate its performance in terms of determining whether it is addressing the intended goal or not. This process of gathering requirements is similar to the *needs and context analysis* phase, as described in the cyclical approach followed by Mckenney and van den Akker (2005:49), which requires a literature review (completed in prior chapters), concept validation (to ensure that the target user group's design requirements are understood), as well as site visits (to validate and gather design requirements) where participatory design workshops will be held with members of the target user group.

The participatory design workshops will be conducted in a similar fashion to those performed in the studies by Anthony *et al.* (2012) and Khaled and Vasalou (2014:95). The two studies were briefly discussed in Section 2.4.2. The key takeaways from those studies, which will be applied to

this study, are that the participatory design workshops will be kept to a manageable size (four participants) and that the requirements will be gathered from the participants through verbal and transcribed methods.

4.2.1 Requirements

Identifying the requirements of the artefact design is crucial as it will guide how it should be presented and improved. This process will ensure the design meets the target user group's expectations. This study follows a participatory design approach, which requires workshops to be performed as a platform to obtain feedback on the design requirements of the artefact. It is imperative to note that the requirements gathering process is described in this section according to the pre-artefact (conceptual design and development) stage, mid-artefact (prototype design and development) stage, and post-artefact (artefact evaluation) stage.

4.2.1.1 Pre-artefact

Before the artefact can be designed, an understanding is needed to determine who the target audience is. Given that the research will involve interaction with people, ethical clearance was obtained from the institution at the start of the study. The individuals relevant to the study will have to be identified and their written consent for participation will have to be obtained. The consent forms will have to be drafted and approved by the study leader. The specific individuals who adequately fall within the targeted audience are identified as administrative staff from medium to large organisations. To communicate the logistics with these individuals, communication platforms such as verbal (face-to-face or telephonic) and email can be used.

Subsequent to identifying the relevant participants, a workshop is set up for a participatory design approach to data collection. The workshop will provide the participants with an overview of what was identified in the literature and what the objectives of this study are. In order for this to happen, a presentation summarising the literature findings needs to be drafted by the researcher and subsequently approved by the study leader. During the workshop, the findings from the literature regarding cyber-security and social engineering issues, which are pertinent to their specific vocations, are presented to the target user participants.

Requirements will be gathered from the participants in order to determine the relevant platform for developing the game-based artefact that suites their needs. The related visual design elements will also be determined. These design elements are determined mainly by the target user group as well as knowledgeable experts (from academia) in the design science research field. The participants relevant to the initial workshop will include administrative staff. Experts within the design science research space will also assist with defining the design guidelines for

the user experience as well as to develop the content relevant to the study. To adequately present the design of the artefact, a needs analysis process will be followed with the participants, which will guide the artefact design. The needs analysis will capture the design elements from the participants in a guided approach, which ensures that the responses remain as relevant as possible. In order to facilitate the creativity of the participants, reference will be made to the artefacts that have already been designed by other researchers (as was discussed in Section 3.2.5). The key concepts of social engineering that need to be highlighted by the game will also be referenced throughout the workshops to facilitate the relevance of the participant responses.

To summarise the above, the process to obtain the requirements for creating the initial conceptual design is as follows (conceptual design process performed in Chapter 5):

1. Obtain ethical clearance from the institution;
2. Identify the target audience;
3. Obtain the target audience's consent to be participants in the study;
4. Introduce the target audience to the study and the literature findings (during workshop 1);
5. Obtain feedback on a suitable platform for presenting a game of this nature (during workshop 1);
6. Obtain feedback on the design elements pertinent to the conceptual design of the game (during workshop 1); and
7. Create a conceptual design based on the feedback obtained and confirm the requirements were correctly captured and translated from workshop 1 (during workshop 2).

Once the initial conceptual design requirements have been obtained, the conceptual design of the artefact will be created and presented to the participants in subsequent workshops. This process will then collaboratively lead to the conceptual design in the form of a mood board and storyboard. The mood board and storyboard (storyboard also referred to as the conceptual prototype) will be used to develop the first prototype (prototype developed in Chapter 6).

4.2.1.2 Mid-artefact

Once the requirements have been gathered and implemented in the conceptual design, the participants will validate the conceptual design (the mood board and storyboard) and the prototype artefact will be created. The prototype design process is limited to two prototype design iterations, which are described.

First prototype design

The first prototype will be designed from the design information contained in the conceptual design. The development of the prototype will go through a series of design cycles made up of a number of activities in each iteration (refer to the example by Heymann and Greeff (2018:16) as depicted in Figure 2-7 under Section 2.5.4). The prototype (during the build process) will be altered to suit the needs of the target audience. Each iteration (circuit) will require a workshop to be presented to evaluate the design and to gather requirements. The requirements will be translated into a set of features that will be built and presented to the experts (from industry or academia). The experts will provide recommendations that will be noted and applied to the design iteration. Once all expert consultations for the design phases have been completed, the design will be presented to the target audience again to evaluate and ensure that the design aligns with their requirements. This process will continue until a usable prototype has been created.

To above first prototype design creation process is summarised as follows:

1. Develop the working prototype from the conceptual design prototype (conceptual prototype design is discussed in Chapter 5);

2. Obtain expert feedback and improve the prototype 1 design (over two prototype development revisions); and

3. Present prototype 1 to participants for feedback in a participatory design workshop (workshop 3).

This will conclude the first prototype design.

Second prototype design

At the start of the second prototype design cycle, the first prototype will be presented (as workshop 3) to a different set of participants who fall within the same target user group (who are administrators in a medium to large organisation). The new participants will provide their feedback about the first prototype, which will be noted, considered, and subsequently applied throughout the iterations of the design cycle. The process followed with the second group of participants will continue in the same manner as it did with the first group. The similarity is that the design of the second prototype is derived from the first prototype and the participant feedback. The participant feedback, in tandem with the experts' feedback, drives the second prototype design.

To summarise the above, the process to create the second prototype design, as an extension of the first prototype design, is as follows:

1. Develop prototype 2 based on the design feedback obtained from the participants (in workshop 3);

2. Obtain expert feedback and improve the prototype 2 design (over two artefact development revisions); and

3. Conclude the artefact design and development, and continue to the artefact summative evaluation and testing phase (performed in Chapter 7).

This will concluded the prototype 2 artefact development that will be released for a summative evaluation and test (which is performed in Chapter 7).

This approach, used to design the conceptual design and prototypes, aligns with that of Mckenney and van den Akker (2005:48), as it involves the participants and involves some form of a design and evaluation element for each prototype created. The testing (described in Section 4.2.2 – testing) of the artefact occurs continuously with the experts and participants throughout the entire artefact design and development process. This is representative of the agile development methodology which is iterative (cyclical) in nature and involves the developers and users of the artefact.

Upon completion of the second prototype, it will be evaluated according to the summative evaluation and testing approach described in Section 4.4.2 (artefact evaluation), which follows two levels of the four-level model for evaluating artefacts.

4.2.1.3 Post-artefact

Any requirements gathered as suggestions for improvement during the post-artefact design phase will be discussed as future research in the final chapter (Chapter 8).

4.2.2 Testing

Testing will be used to determine whether the inputs to the design science research process were adequately defined and translated, and whether design improvements can be made according to expert feedback. Testing applies throughout all the development iterations of the artefact. Testing specifically refers to interaction with the artefact by the design experts to determine whether any improvements should be made or whether the artefact can be evaluated. It is important to remember that a formal evaluation of the artefact (as defined in Section 4.4.2) can only occur once the experts confirm that the artefact has reached a state good enough to present as summative evaluation and testing approach to the target user participants.

4.2.2.1 Artefact testing

Experts (from academia) will continuously be involved in the artefact testing process to provide guidance on the artefact design as it relates to game-based design as well as any context-specific requirements that emerge. The test results for the conceptual artefact are briefly described in Sections 5.2.2, but the detailed results are described as part of the design and development iterations described in Sections 5.3.1.1 to 5.3.1.4. The test results for the prototype artefact are also briefly described in Section 6.3.2, but the detailed results are depicted in Section 6.4.1.1 to 6.4.1.5 as part of the design and development iterations. No testing is applicable to Chapter 7 as the artefact development has stopped (at the end of Chapter 6) and the artefact is being evaluated through a summative evaluation and test.

The testing performed in Chapter 5 by the experts (from academia) tests adequacy for the following specific outcomes (over a total of four iterations):

- The PowerPoint presentation design;
- The consent forms design;
- Mood board 1 design;
- Mood board 2 design; and
- The conceptual prototype design.

The testing performed in Chapter 6 by the experts (from academia) tests adequacy for the following specific outcomes:

- The prototype 1 design (over three iterations); and
- The prototype 2 design (over two iterations).

4.3 Rigor cycle

For the rigor cycle, the research will be grounded on scientific theories and expertise based on prior knowledge to ensure design innovation. The design cycle will reference the rigor cycle to ensure that the design does not deviate from the scientific methodologies that have already been established in prior research. From following these established methodologies, existing knowledge or processes will be validated, or in the case where this is not valid, the new knowledge or processes gained will be communicated and will form additions to the knowledge base.

4.3.1 Grounding

The design of the artefact is grounded in design science research principles as per the design science research methodology (DSRM) process model by Peffers *et al.* (2007:54) (discussed in Section 2.4.1.2). The secondary objectives for the study were defined according to the phases of the DSRM process model as was discussed under Section 2.5.1.1 in Table 2-17.

4.3.1.1 Pre-artefact

The research is grounded in design science research methods and also in the literature. The literature provided detail regarding some of the available research paradigms and research methods. The literature also provided detail of design science research and covered areas pertaining to research frameworks (discussed in Section 2.4.1), design guidelines (discussed in Section 2.4.3) as well as how to evaluate and report on the design (discussed in Section 2.4.4). The development of the conceptual design (pre-artefact) is grounded in design science research cycles by Hevner (2007:2). The state of cyber-security with a key focus on social engineering as well as the applicability of games as a teaching aid were also covered in the literature (discussed in Chapter 3).

4.3.1.2 Mid-artefact

For the purpose of this study, the development guidelines of the prototype design (mid-artefact) will be grounded in the design science research experts' knowledge. The relevant literature, in tandem with the participants' needs, will guide the design of the artefact. The relevant literature that will support the requirements and needs of the design and development of the artefact will be sourced as these requirements and needs are identified. As with the pre-artefact, the mid-artefact is also grounded in the design science research cycles by Hevner (2007:2). The grounding may also include updated DSR theory, appropriate examples of social engineering attacks, or design guidelines for game-based artefacts.

4.3.1.3 Post-artefact

The final evaluation of the completed artefact will be grounded in the literature that describes the testing and evaluation of artefacts of this nature. The summative evaluation and testing of the artefact will be grounded in the ***reaction*** and ***learning*** evaluation levels by Petri and von Wangenheim (2016:995) (refer to Table 2-11 in Section 2.4.2, which depicts the four-level model for evaluating educational artefacts) and excludes the ***behaviour*** and ***results*** levels – this is due to the nature of this study and time constraints. The design science research checklist by Hevner and Chatterjee (2010a:20) will be used to communicate the success of this study (checklist briefly

discussed in Table 2-15 under Section 2.4.4). The reporting of this DSR study (discussed in Section 2.5.4) will be grounded in the research by Mckenney and van den Akker (2005:48), which highlighted the quality aspects for designing, developing and evaluating an artefact.

4.3.2 Additions to knowledge base

Additions to the knowledge base will occur throughout the phases of the design, development, and evaluation of the artefact. This will be either in the form of validation of what is already existing in the knowledge base, or through new additions arising from experiences that did not exist in the literature (also as literature contributions).

4.3.2.1 Pre-artefact

Tools and techniques that will be used to gather requirements and understand the context, i.e. questionnaires, PowerPoint slides, etc. will need to be identified. These tools and techniques will be used to obtain the necessary information to gather data that will be evaluated. The tools and techniques that are used to convey concepts to the participants will be described and can be noted as additions to the knowledge base. Additionally, the tools used to create the conceptual design will also be described and can possibly contribute new knowledge to the knowledge base. Excerpts from the findings in this section of the study can be added as potential literature publications.

4.3.2.2 Mid-artefact

During the prototype design of the artefact, a series of technique additions to the knowledge base will be relevant to the practitioner knowledge base. These new knowledge contributions will be beneficial to practitioners who make game-based artefacts. Additions with regard to the ease of adapting changes in the artefact through the evaluation phases will also be noted and will contribute to the knowledge base. Any other additional knowledge that is identified during the design process can possibly be added to the knowledge base. Excerpts from the findings in this section of the study can be added as potential literature publications.

4.3.2.3 Post-artefact

Post-artefact contributions to the knowledge base will be in the form of the testing of the effectiveness of the artefact within the specific context. Any new techniques identified during the testing and evaluation of the artefact, which were not previously identified in the literature, can contribute to the research body of knowledge. Any findings from the testing results can also be noted as contributions to the research body of knowledge.

4.4 Design cycle

It is important to bear in mind that the design cycle is strongly dependent on the *relevance* and *rigor* cycle of the DSR cycles by Hevner (2007:2). These two cycles have an important role in driving the iterative design of the artefact. This means that the requirements are input from the *relevance* cycle, while the design and evaluation theories and methods are extracted from the *rigor* cycle. The design cycle is iterative in nature and is similar to the process of *design, development, and formative evaluation* of the Mckenney and van den Akker (2005:49) iterative cycles, where one or more prototypes are developed based on specific design requirements. The prototype is subsequently evaluated based on a set of criteria to ensure that the design meets its requirements or targeted results.

4.4.1 Artefact design

This section of the design cycle determines how the artefact will be designed and developed. It describes the cyclical and iterative processes that will be followed in building the conceptual artefact as well as the prototype designs. The artefact design process will undergo a process similar to that used by Heymann and Greeff (2018:498), which is depicted in Figure 4-3.

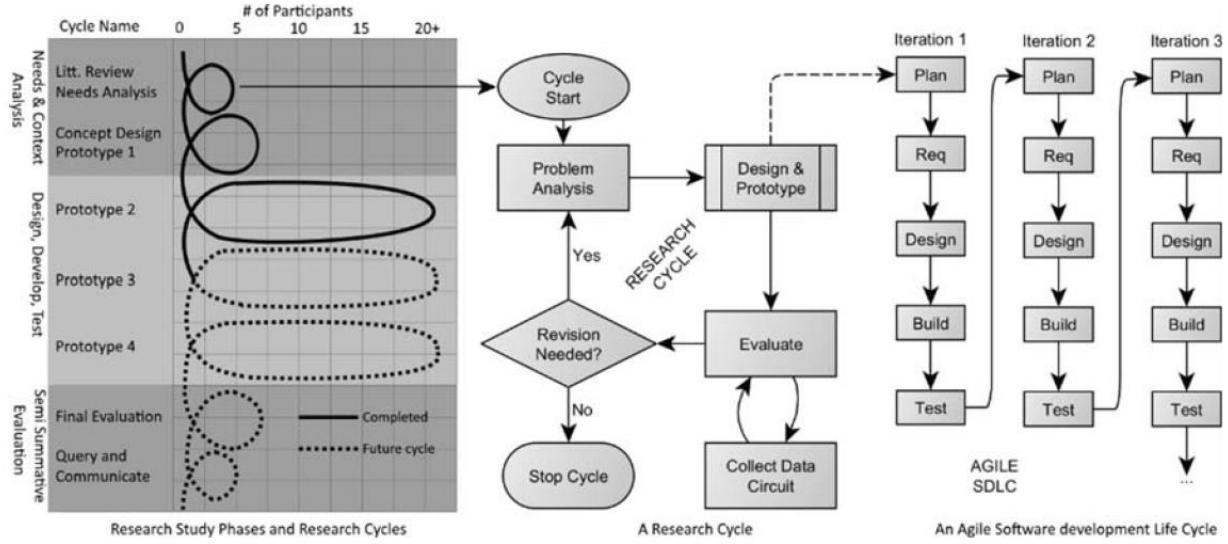


Figure 4-3: The Mckenney and van den Akker (2005:49) research cycles as followed by Heymann and Greeff (2018:498)

4.4.1.1 Pre-artefact

The conceptual design will follow the Mckenney and van den Akker (2005:49) cyclical approach for *designing, developing, and evaluation* of the conceptual artefact. The conceptual design of the

artefact will be created using mood boarding and story boarding. The requirements gathered from the target user group, within the specific context being studied, as well as what is in the literature, are what drives the need for artefacts of this nature. These factors also drive the requirements for developing the artefacts. The conceptual design is the starting point for an initial prototype design that will provide the target user group with an idea of what the end-product could possibly look like, and consequently allows the target user group to provide further feedback on improving the design.

It is important that the appropriate application(s) for designing and developing the conceptual design are adequately identified as they will need to sufficiently represent the specific requirements that were obtained from the target user group. Once done, the mood board and storyboard can be created using the design elements identified from the themes presented. Design expert (from academia) feedback can also be used to refine the design of the conceptual artefact.

4.4.1.2 Mid-artefact

As with the conceptual design, the prototype design will also follow the Mckenney and van den Akker (2005:49) cyclical approach for *designing, developing, and evaluation* of the prototype artefact. Based on the scope of the study, multiple iterations of the design, development, and formative evaluation phase for the prototype design will be followed. Figure 4-4 depicts an example of the process.

The first prototype will be created in a suitable game development platform that is based on the elements identified in the pre-artefact requirements gathering phase. The prototype design will be directed by the conceptual design as well as the workshops that will be held with the target user group to ensure that the artefact is designed according to their requirements. Additionally, the design science research experts will be continuously involved in the artefact design and development process, providing experienced design input to the design. Where a particular section of the development cannot be done by the researcher, predefined assets will be acquired and modified for the artefact.

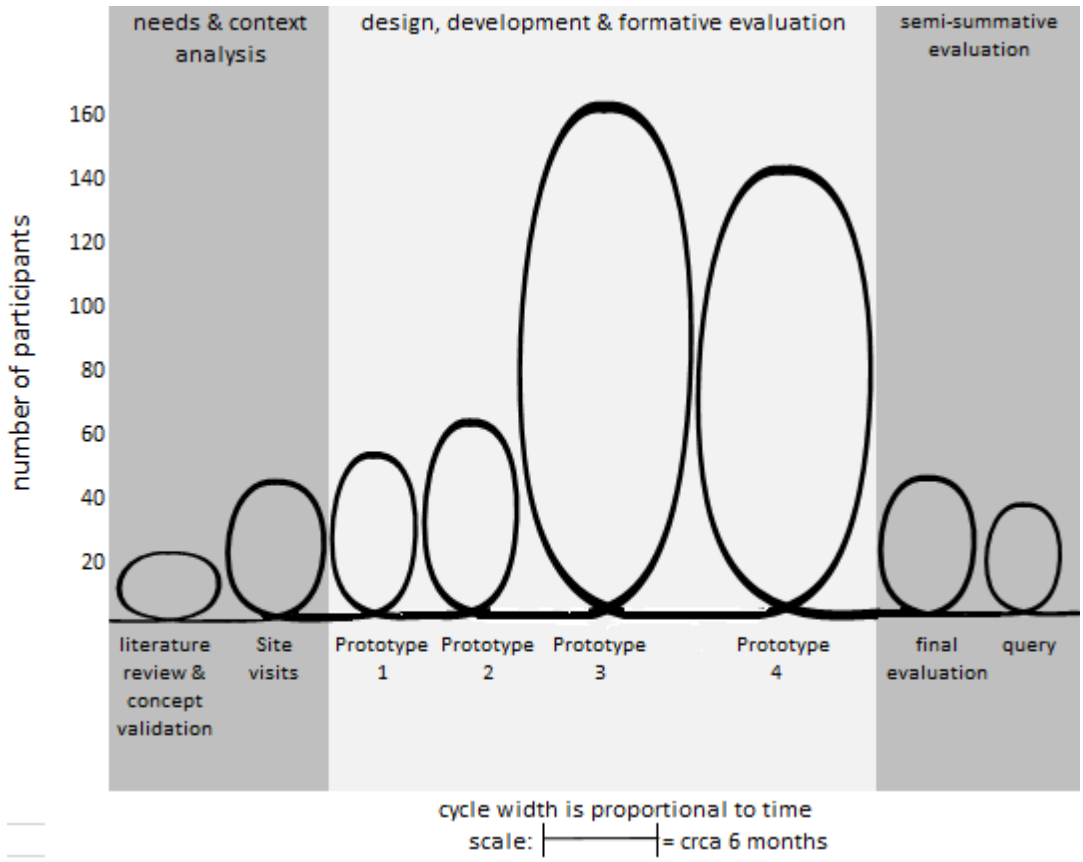


Figure 4-4: Cyclical approach to the three phases followed by Mckenney and van den Akker (2005:49)

The section that follows will discuss the post-artefact design approach.

4.4.1.3 Post-artefact

Post-artefact implies that the artefact has been completed and that no additional post-artefact design processes are necessary. However, the artefact design will be tested and evaluated at this stage through a summative evaluation and testing approach to ensure that it reflects the design requirements defined in the *relevance* cycle.

4.4.2 Artefact evaluation

This section of the design cycle determines how the artefact will be evaluated throughout each design iteration as mini evaluations (which are referred to as the artefact evaluations) and a final summative evaluation and testing approach.

It is very important that these mini evaluations are not confused with the summative evaluation and testing. The summative evaluation and test is a comprehensive evaluation of the artefact to

determine how the target user group feels about the artefact (***reaction*** evaluation) and whether the artefact can bring about a learning experience in the participants (***learning*** evaluation). The mini evaluation sessions are specifically geared at allowing the target user group participants to see and interact with the artefact. We will refer to these mini evaluations only as artefact evaluations throughout this study with the summative evaluation and testing also being clearly distinguished.

The artefact will therefore be evaluated from the conceptual design (pre-artefact), to the prototype design (mid-artefact), and will undergo a summative evaluation and test (post-artefact) to determine whether the intended objectives of the study were addressed.

4.4.2.1 Pre-artefact

During the design cycle, the conceptual design will be evaluated by the target users in participatory design sessions. These artefact evaluation sessions will happen at regular intervals to ensure that the design is usable for the targeted user groups. The sessions will be conducted with the participants from Company A to allow their views and opinions to guide the design and development of the artefact. The evaluation at this stage does not follow a specific evaluation criteria.

4.4.2.2 Mid-artefact

As with the pre-artefact, the prototype 1 and prototype 2 will be evaluated by the different target users in a participatory design session. The session will be with participants from Company B. The evaluation at this stage does not follow a very specific evaluation criteria.

4.4.2.3 Post-artefact

Once the working prototype artefact (prototype 2) development process has been completed, it will be measured for performance within the context for which it was designed. It will be measured by the target user group as well as well as other users who do not necessarily fall within the target user group. It is important to note that the post-artefact evaluation process will occur in the form of a summative evaluation and test. The summative evaluation involves a ***reaction*** and ***learning*** evaluation of the artefact. The artefact will also be evaluated for quality using a set of quality evaluation criteria by Mckenney and van den Akker (2005:48) which were depicted in Table 2-13 under Section 2.4.4.4.

This section describes the post-artefact evaluation approach. It occurs as a summative evaluation and test which follows two levels from the four-level model by Petri and von Wangenheim (2016:995). Due to the nature of this study, only the ***reaction*** and ***learning*** levels of the artefact

evaluation will be performed. This is due to the process followed in the development of the artefact. The artefact is only intended to be evaluated as a once-off assessment at the end of its development and not where it is used in practice over an extended period. The *behaviour* and *results* evaluation levels require that the artefact be assessed over an extended period, which does not fall within the scope of the study.

For the ***reaction*** level in the evaluation model, the participants will be provided with feedback forms that assess the experience they had when interacting with the game. The participants will be the users that formed part of the previous conceptual and prototype design workshops. The feedback forms will determine whether the participants' design requirements were adequately addressed and what additional requirements they would have liked to see. This feedback will be obtained after the participants have interacted with the artefact and will be used in future research.

For the ***learning*** level in the evaluation model, only participants who were not involved in any of the design and development workshops will be included. The participants will undergo a pre- and post-test questionnaire. The pre-test questionnaire will be provided to the participants regarding social engineering concepts to determine their initial level of understanding. The intention was to present both the questionnaires in a participatory design workshop, but due to the COVID-19 pandemic, the questionnaires will be delivered electronically to the participants. The artefact will then be presented to the participants and will be followed by a post-test questionnaire. The results from the questionnaires will be compared to determine whether a learning experience occurred after participants have interacted with the artefact.

Both forms of the ***reaction*** and ***learning*** evaluation were intended to be presented in a fourth participatory design workshop, but due to the COVID-19 pandemic, they will be delivered electronically to the participants

The second prototype design will also be evaluated for quality against a set of quality aspect similar to those defined by Mckenney and van den Akker (2005:48) for *designing, developing, and evaluating* an artefact (depicted in Table 4-1).

Table 4-1: Quality aspects for designing, developing, and evaluating the CASCADE-SEA program (Mckenney & van den Akker, 2005:48)

	Traits / Quality	Content	Support	Interface
Validity	State-of-the-art knowledge	Curriculum design and development knowledge; Related	Advice on materials design; Guidance on embedding materials in	Maximise the potential of modern ICT facilities

	Traits / Quality	Content	Support	Interface
		professional development knowledge	professional development	
	Internally consistent	Ideas in various components are in line with those in other areas	Tips guidelines, templates, advice, and help functions are perpetually offered in a consistent fashion	Functions as intended, regularly
Practicality	Instrumentality	Guides the user step-by-step in making materials; offers freedom to work at own pace and in own style	Explains how to use program clearly and concisely	Buttons, navigation, and functions are clear
	Congruence	Links up with the needs, wishes and context of the users	Support is relevant and usable	Interface 'feels' nice and safe, users are not alienated, but motivated to use the program; Operates on technology that is available in the target setting
	Cost	Content should include enough of what users need, and not hog them down with unnecessary steps	Support should be extensive, lowering the threshold of investment cost of the user	Interface should reflect the flexibility of the system, in which users determine how they would like to go through the program (maximum degree of freedom, minimum allowance for error)
Impact potential	Yields better quality materials	The materials that are developed through the use of the CASCADE-SEA should be valid, practical, and effective	The materials that are created with the CASCADE-SEA should contain clear, useful procedural specifications	The materials that are generated with the CASCADE-SEA should evidence attention given to form and style
	Enhances the professional development of users	CASCADE-SEA should help users to think about the materials development in a (more) systematic and thorough fashion	Teaches users where resources can be found (inside the program), and how they may be used and/or adapt for own setting	Interface helps (teams of) user to visualise the process of materials development and make their work more transparent

The artefact quality evaluation will conclude the artefact evaluation approach. The ***reaction*** level evaluation results will be discussed in Section 7.3.1. The ***learning*** level evaluation results will be discussed in Section 7.3.2. The ***quality*** evaluation results will be discussed in Section 7.3.3.

4.5 Conclusion

This section discussed the DSR cycles by Hevner (2007:2) and how they will guide the development of the artefact in this study. From this, the methods to obtain the artefact design

requirements were identified. The guidelines on how the design requirements will be translated into a conceptual design were described. The guidelines that will be used in translating the conceptual design into a prototype design were also described. And finally, the process that will be used to evaluate the conceptual and prototype design as a summative evaluation and testing process were also discussed.

The summative evaluation and testing of the prototype follows the ***reaction*** and ***learning*** evaluation levels and also evaluates the *quality* of the artefact design. The reaction and learning evaluation levels are from the four-level model to evaluate game-based artefacts by Petri and von Wangenheim (2016:995). This limitation was discussed in Section 4.3.1.3. The Mckenney and van den Akker (2005:49) cyclical approach was discussed and the process of how it will be used in this study to guide the prototype design. An example of the cyclical approach that will be followed was further demonstrated by Heymann and Greeff (2018:498), which was illustrated in Figure 4-3, Section 4.4.1. The *quality* of the artefact will be evaluated using the evaluation criteria by Mckenney and van den Akker (2005:48) (discussed in Section 4.4.2.3 and depicted in Table 4-1), which relates to the quality aspects for *designing, developing, and evaluating* an artefact.

The grounding of the prototype design will be based on the design science research principles from the design science research methodology (DSRM) process model by Peffers *et al.* (2007:54).

Additions to the knowledge base will occur throughout the design of the artefact, either as validations or identifications of new processes, tools, methods, etc. that arise throughout the design, development, and evaluation of the artefact. Additions to the knowledge base may also be in the form of research publications.

Chapter 4 has provided an outline of how the artefact will be developed and evaluated. Chapters 5 to 7 will document the process followed as described in the outline specified in this chapter. Chapter 5 will discuss the pre-artefact (conceptual design) design and development cycles. Chapter 6 the mid-artefact (prototype design) design and development cycles. Chapter 7 the post-artefact (artefact summative evaluation and testing) cycle.

CHAPTER 5: PRE-ARTEFACT

5.1 Introduction

The primary objective of this study is to design and develop an artefact that can be used to raise awareness about social engineering attacks among administrative staff in medium to large organisations. This chapter will support this primary objective by describing the process that is followed in designing and developing the conceptual artefact.

This chapter follows the pre-artefact design guidelines that were set out in Chapter 4. The goal of this specific chapter is to document the development of a conceptual design that will subsequently guide the design of a working prototype.

The process for obtaining the requirements for creating the initial conceptual design is summarised as follows:

1. Obtain ethical clearance from the institution;
2. Identify the target audience;
3. Obtain the target audience's consent to be participants in the study (during workshop 1);
4. Introduce the target audience to the study and the literature findings (during workshop 1);
5. Obtain feedback on a suitable platform for presenting a game of this nature (during workshop 1);
6. Obtain feedback on the design elements pertinent to the conceptual design of the game (during workshop 1); and
7. Create a conceptual design based on the feedback obtained and confirm the requirements were correctly captured and translated from workshop 1 (during workshop 2).

These steps form part of the conceptual design and are addressed in this chapter according to the DSR cycles by Hevner (2007:2), which is mainly composed of the *relevance* cycle, the *design* cycle, and the *rigor* cycle.

The *relevance* cycle describes the relevance of designing the artefact and describes the requirements for building the conceptual artefact and the testing thereof. The *design* cycle describes the process for developing the artefact; no testing of the artefact by the participants occurs at this stage, as the participants cannot interact with the artefact. Only the experts (from

academia) provide testing feedback on the presentation design, mood board design, and conceptual prototype. The *rigor* cycle describes the grounding that guides the development of the artefact. The *rigor* cycle also takes note of any contributions that can be made to the research knowledge base.

5.2 Relevance cycle

A gap was identified in the literature regarding cyber-security issues that affect the sub-Saharan regions, South Africa in particular. A need was identified to educate administrative staff (the target user group) regarding social engineering attacks. This need would be addressed through the design of a game-based artefact.

The requirements necessary for building the conceptual design of the artefact are gathered, and key criteria that can be used to test the design are identified during the participatory design workshops. These are important to determine whether the conceptual design of the artefact is being designed in-line with the requirements specified by the target audience.

5.2.1 Requirements

In order to satisfy the requirements gathering portion of this study, the target audience is identified. The target audience is specifically administrators from medium to large organisations. The reason for choosing these individuals is mainly because they are more suitable for this study in that they are the most likely candidates to be vulnerable to social engineering attacks, and they meet the constraint of being part of a medium to large organisation. Application for ethical clearance from the institution was obtained prior to the study in order to conduct participatory design workshops with the participants. Participants from one organisation (Company A) who are suitable as the target user group for the participatory design are identified and an email communication is sent out to determine whether they would be available to participate in the study workshop, and when they would be available to participate. The participants availed themselves and an email communication is sent regarding the specifics of the workshop. During the workshop, consent forms are provided to participants as part of the ethical requirements.

The requirements of the conceptual design are gathered from the target audience in two separate workshops. The first workshop is held to gather the initial requirements for developing the first conceptual artefact. The second workshop is to confirm whether the requirements gathered in the first workshop are correctly translated into the conceptual design. During the process of translating and developing the conceptual design, input regarding the design is obtained from various sources, such as the participants from the target user group, as well as the research

experts (from academia). An overview of all participants who formed part of this iteration can be found in Appendix D.

The tools necessary for the conceptual design are identified. Microsoft PowerPoint is used to present a slideshow in order to provide context to the participants, for the first workshop, regarding the purpose of the study as well as crucial concepts relevant to the study (e.g. cyber-security and social engineering). A mobile device is used to voice record responses from the participants to ensure that any points that were not noted during the workshops can be re-evaluated at a later stage. Microsoft OneNote is used to capture notes during discussions with the experts as well as the responses from the participants during the workshops.

Microsoft Word is a tool that can be used to develop the mood board as it can be used to create overlapping images necessary to depict the conceptual design. Twine version 1.4.2 is selected for the development of the storyboard (as a conceptual prototype) as opposed to Twine version 2.3.2; this is due to functionality limitations of Twine 2.3.2. The Twine storyboard images, which are free for use, are obtained from the Unity asset store and modified using Microsoft Paint. In the Unity assets license agreement, Section 2.2, it indicates that end-users may modify Unity assets, as long as they are not restricted assets (Unity, 2020). None of the assets used in this study are restricted. The images captured from the Unity store are selected to closely meet the design requirements that are identified by the participants, which are then translated to the mood board. These images are useful in that a decision is made that predefined assets would be used to fill the artefact design gap where appropriate.

5.2.2 Testing

During the design testing phase, testing is performed with the academia experts. The academia experts provide confirmation whether the PowerPoint presentation that would be presented in workshop 1 is designed adequately. Confirmation that the consent forms are adequately drafted and in-line with the institution's ethical requirements is also obtained form the academia experts. Testing also confirms whether the mood board and conceptual prototype are adequately designed.

5.3 Design cycle

The design of the artefact follows a similar approach as that of the Mckenney and van den Akker (2005:48) and the Heymann and Greeff (2018:498) studies. The *design* cycle for this section of the study aims to develop the conceptual artefact. Figure 5-1 provides a summarised view of the cyclical approach that is followed (in this section of the study) for the design and development of the conceptual artefact. The design and development of the conceptual design are mainly guided

by the requirements gathered from the participants (during the participatory design workshops) as well as the design input received from the experts (during the artefact testing stages) throughout the development process.

Figure 5-1 depicts the *phases*, the *cycles* (iterations) that occur at each phase, as well as the *number of participants* that are involved in each cycle for development of the conceptual artefact. In each of the artefact design and development cycles (iterations), an iterative approach is followed that requires that the artefact *problem* be identified, that the *design* is developed through a technical approach that involves *planning*, gathering the *requirements* for the artefact, *designing* it, *building* it, then finally *testing* it. Testing will determine whether the process will be repeated from the planning step or whether the process can continue to the *evaluation* of the artefact. A decision can then be made whether the *problem* step should be started again or whether the cycle can *stop*. This approach is similar to an agile development methodology in that it closely involves the end users and developers throughout the development process (Cordeiro *et al.*, 2007:197).

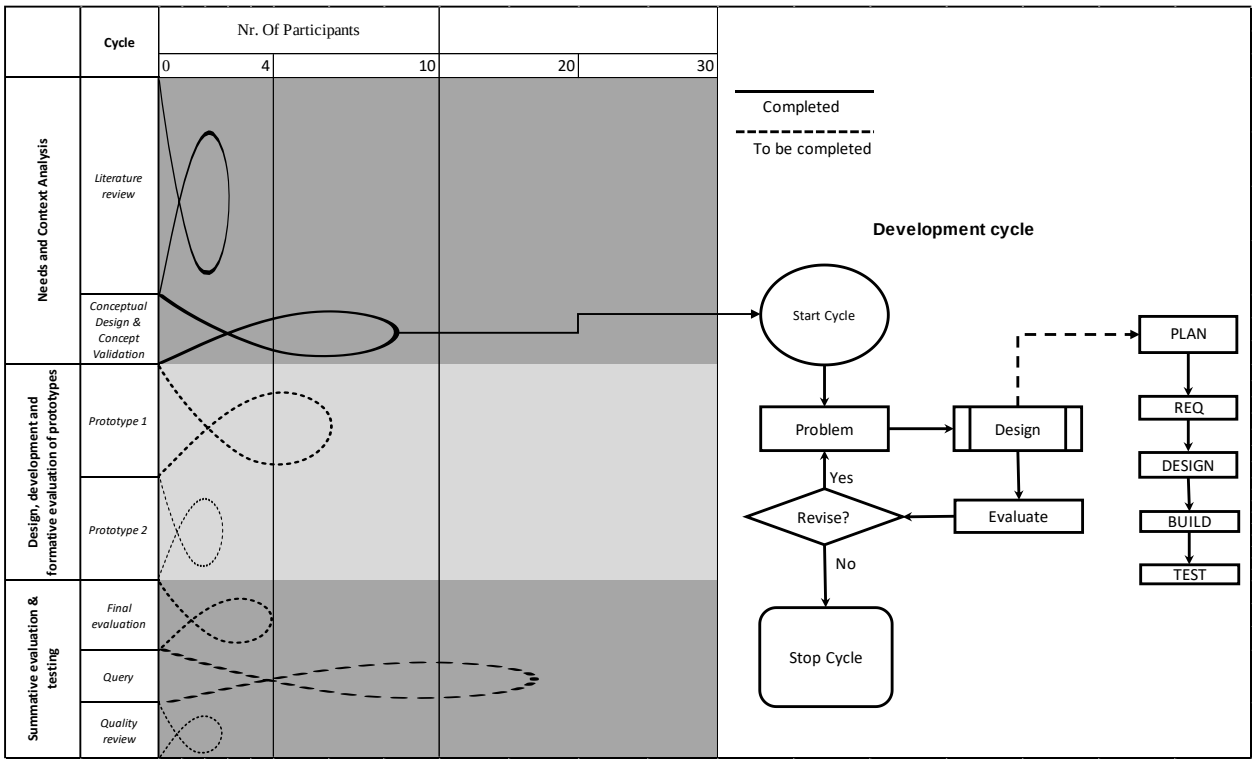


Figure 5-1: Research cycle for the conceptual design of the artefact

To avoid confusion, Table 5-1 contextualises the design and development process for the conceptual design (mood board and conceptual prototype), as well as the prototype artefact (prototype 1 and prototype 2). It is also summarised as an illustration depicted as Figure 5-2. It is

important for context that these two summaries are examined before reading into the artefact design and development detail. This information is intentionally presented early in this section for the work that still needs to be discussed over Chapters 5 to 7, primarily for the reason of providing the reader with an enhanced view of the cyclical process that will follow, which may become difficult to follow without this context.

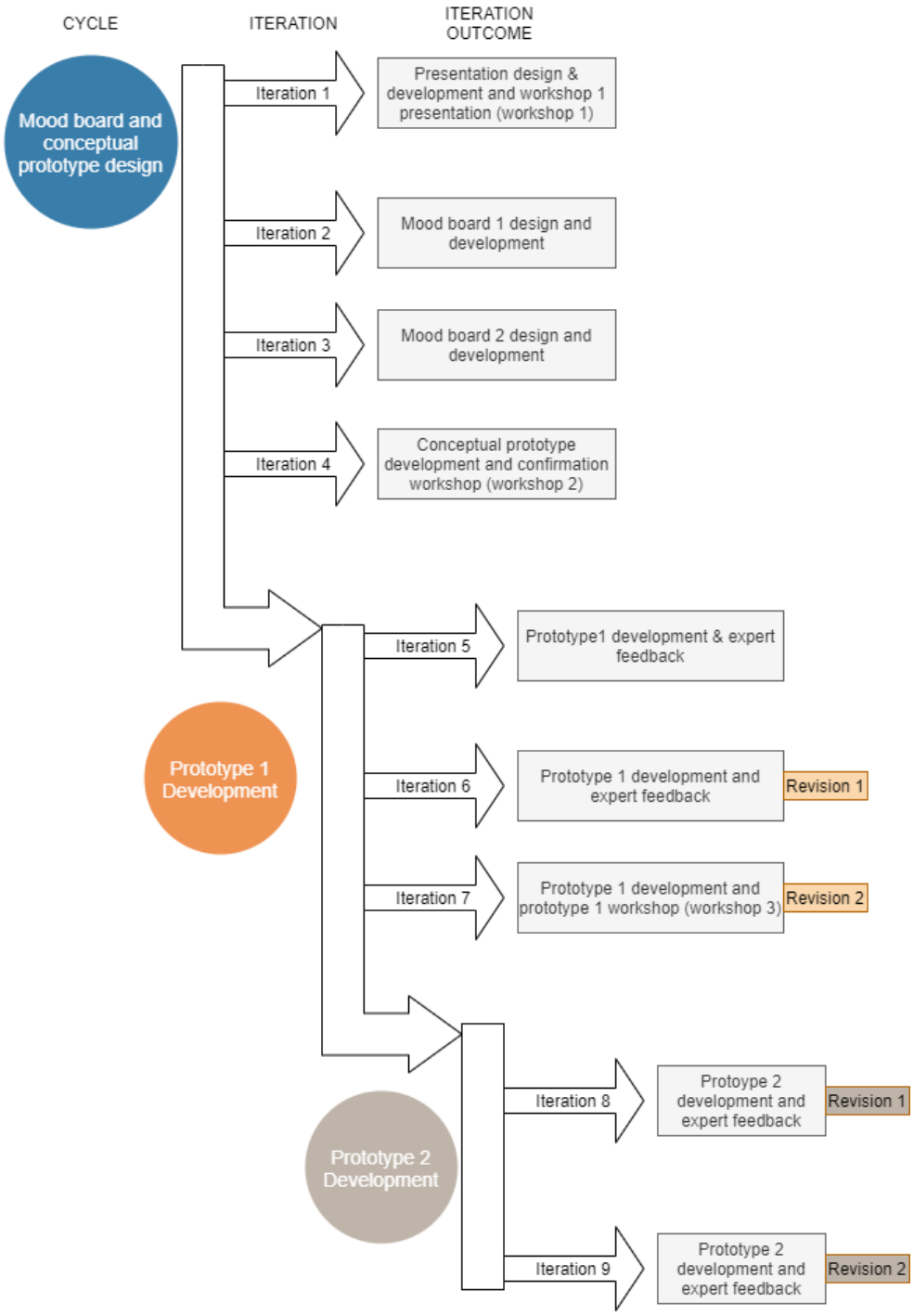


Figure 5-2: A summary of the artefact development iterations

Table 5-1: Summary and contextualisation of the artefact development iterations

Cycle	Iteration	Table ref.	Revision	Iteration outcome
Conceptual design & concept validation	1	Table 5-1	N/A – The revisions with the experts are not documented as the feedback is brief. This applies for iterations 1-4.	Presentation design and development. Workshop 1 presentation.
	2	Table 5-2	N/A	Mood board 1 development.
	3	Table 5-3	N/A	Mood board 2 development and conceptual prototype development.
	4	Table 5-4	N/A	Conceptual design (mood board 2 and conceptual prototype) confirmation workshop (workshop 2).
Prototype 1	5	Table 6-2	N/A – No revision in this iteration as development work happens first (there is no prototype to revise at this point). Experts evaluate the artefact at the end of the development work and therefore, Table 6-4 describes the results from the experts' revision as revision 1.	Prototype 1 development. Expert feedback (as revision 1) at the end of the development iteration.
	6	Table 6-4	Revision 1.	Prototype 1 development using revision 1 results. Expert feedback at the end of the development iteration as revision 2.
	7	Table 6-5	Revision 2.	Prototype 1 development using revision 2 results. Prototype 1 workshop (prototype 1 test as workshop 3).
Prototype 2	8	Table 6-8	Revision 1.	Prototype 2 development using iteration 7, revision 2 results. Expert feedback at the end of the development iteration as revision 2.

Cycle	Iteration	Table ref.	Revision	Iteration outcome
	9	Table 6-9	Revision 2	Prototype 2 development using iteration 8, revision 1 results. Expert feedback at the end of the development iteration. However, no specific revision results are documented as the results from the expert feedback are minimal. Proceed to artefact summative evaluation and test phase.

This cycle (conceptual design & concept validation) consists of four iterations. *Iteration 1* is the design of the presentation, *iteration 2* is the development of mood board 1, *iteration 3* is the development of mood board 2, and *iteration 4* is the development and confirmation of the conceptual design. Chapter 6 will discuss the development of prototype 1 and prototype 2. Prototype 1 is a first attempt at translating mood board 2 and the conceptual prototype into a working artefact (as iteration 5 to 7). Prototype 2 is an improvement of prototype 1 (as iteration 8 and 9). Chapter 7 will discuss the ***reaction*** and ***learning*** evaluation of the working prototype 2.

5.3.1 Artefact design

This section will discuss the conceptual artefact design process. An overview is provided on the four iterations that form part of this cycle.

5.3.1.1 Iteration 1 (presentation design)

In iteration 1, the requirements for developing the conceptual design are obtained from the participants. During the first participatory design workshop, four target user group participants from Company A provided feedback on design requirements (see Appendix D for an overview of participants). Table 5-2 depicts the agile process that was followed for iteration 1.

Table 5-2: Iteration 1: Presentation design process

Cycle	Activity
Problem	The problem identified in this iteration was to determine how information regarding social engineering and some of the artefacts developed in research, could be presented to the target user group. The need for presenting the information to the participants was to obtain feedback regarding the artefact design requirements.

Design	Plan	Planning for the development of the presentation required the following action items to be performed: • Build a presentation to present cyber security and social engineering issues, along with the artefacts identified for raising social engineering issues; and • Draft consent forms and obtain participant consent.
	Requirements	The following tools were required to build the presentation and obtain consent from the participants: • Microsoft PowerPoint as a tool to present the information; and • Microsoft Word as a tool to draft participant consent forms.
	Design	The following design elements were identified to develop the tools that would be used to obtain the design information from the participants regarding the development of the artefact: • Draft a layout of the items to be discussed during the participatory design workshop; • Obtain PowerPoint presentation design guidance from the DSR experts; and • Obtain guidance regarding the consent form design and ethical requirements from the DSR experts.
	Build	The following items were built for the presentation to the participants: • A PowerPoint presentation explaining the social engineering issues which were identified in the literature; and • Ethical clearance forms.
	Test	The following design testing was performed with the academia experts: • Confirmation that the PowerPoint presentation is designed adequately; and • Confirmation that the consent forms are drafted adequately in-line with the institution's ethical requirements.
Evaluate		A PowerPoint presentation (containing the social engineering issues and identified artefacts) was presented to the participants. Feedback was obtained regarding the design requirements that would be suitable for developing a game-based artefact that can be used to raise social engineering awareness among administrative staff. The feedback was open-coded to identify themes in the data. These themes included requirements for the type of platform, the character, the game mechanics, and the user interface design. Detailed codes can be found in Appendix E.
Revise		Yes. A revision is necessary in order to translate the design requirements into a mood board.

5.3.1.2 Iteration 2 (mood board 1 design)

In iteration 2, a first conceptual mood board is developed by the researcher and evaluated by two design science research experts and a design artist (from academia). A mood board is required to graphically depict the identified design requirements. The mood board can then be used to

verify (with the target user group participants) that the design requirements were understood. Table 5-3 depicts the agile process that was followed for iteration 2.

Table 5-3: Iteration 2: Mood board 1 design process

Cycle		Activity
Problem		The problem identified in this iteration was to develop a mood board that graphically translates the design requirements gathered from the participants during iteration 1.
Design	Plan	Planning for the development of the mood board required the following action items to be performed: • Obtain an understanding through internet searches and design experts on how to design a mood board; and • Obtain design elements that align to the design requirements identified in iteration 1 (workshop 1) that can be used in the development of the mood board.
	Requirements	The requirements for developing the artefact required understanding design elements such as the visual resources that depict the mood board design, understanding the platform requirements on which the mood would be created, etc. The requirement for building the mood board could be performed using platforms such as Microsoft PowerPoint, Microsoft Paint, Image editor, Microsoft Word, etc. Microsoft Word was the chosen platform as it can be used to create collages and overlapping images for mood board development. The coded themes (refer to Appendix E) such as the artefact platform, character, mechanics, and user interface design requirements from the iteration 1 workshop with the participants are used to design the artefact.
	Design	The following design elements were identified for the development of the mood board: • Visually grouping design elements in such a way that they can tell a story; and • The design experts provide advice on the applicable mood board design elements.
	Build	Build mood board 1 (refer to Figure 5-3).
	Test	Testing is performed by confirming, with the design science research experts and a design artist, that the mood board is designed adequately (refer to Appendix F for the expert feedback and recommendations). Design issues such as the colour palette, related concepts, and inappropriate design elements were highlighted and a redesign was requested.
Evaluate		Evaluation is not applicable as the mood board's design is not adequate to present to the participants.
Revise		Yes. A revision is necessary as the mood board 1 design is not adequate.

Figure 5-3 depicts the design of the first mood board. The design experts indicated that the design was not adequate and needed to be revised in a next iteration before it could be presented to participants.

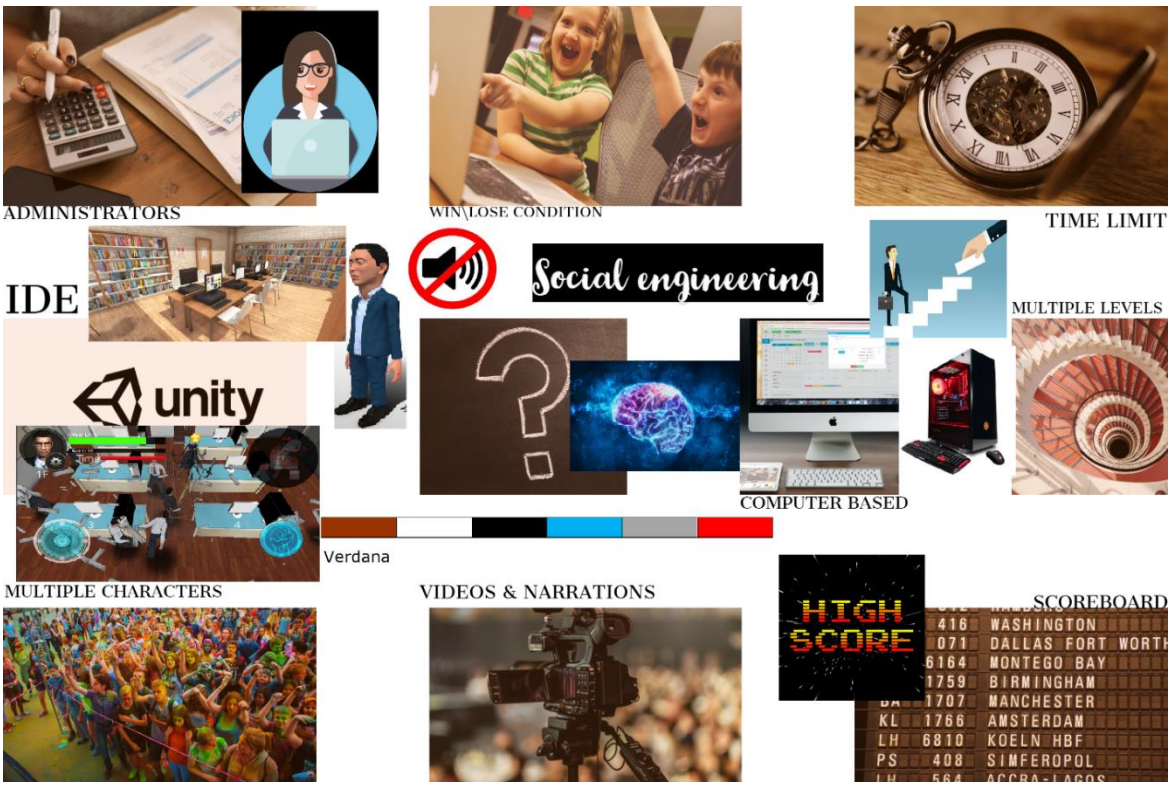


Figure 5-3: First conceptual mood board design

5.3.1.3 Iteration 3 (mood board 2 design)

Iteration 3 yields a second and improved mood board based on the feedback obtained from the design experts. Table 5-4 depicts the agile process that was followed for iteration 3.

Table 5-4: Iteration 3: Mood board 2 design process

Cycle		Activity
Problem		The problem identified in this iteration was to revise mood board 1 with guidance from the design experts (design science research experts and a design artist).
Design	Plan	Planning for the revision of mood board 1 was as follows: • Obtain appropriate design elements that more closely represent the specified design requirements; • Develop mood board 2 (improvement from mood board 1); and • Obtain guidance from the research experts on the mood board 2 design.
	Requirements	The requirement for building mood board 2 was to continue the use of Microsoft Word as a mood board development platform.
	Design	The mood board 2 requirements for the design elements were outlined by the design experts (refer to Appendix F). The mood board 1 design elements were also referred to where appropriate.

	Build	Build mood board 2 (refer to Figure 5-4).
	Test	Testing is performed by confirming with the design experts that mood board 2 is designed adequately.
Evaluate		Evaluation was not applicable yet, as the development of a conceptual prototype of the storyboard was first required before the second workshop with the participants. Mood board 2 will be evaluated along with the conceptual prototype in iteration 4.
Revise		Yes. According to the design experts, the revised mood board was adequate after iteration 3; however, a conceptual prototype still needs to be developed before workshop 2.

Figure 5-4 depicts the design of the second mood board. Design experts indicated that mood board 2 represented the design requirements more accurately, and that a conceptual prototype could be developed using mood board 2 as a design guideline.

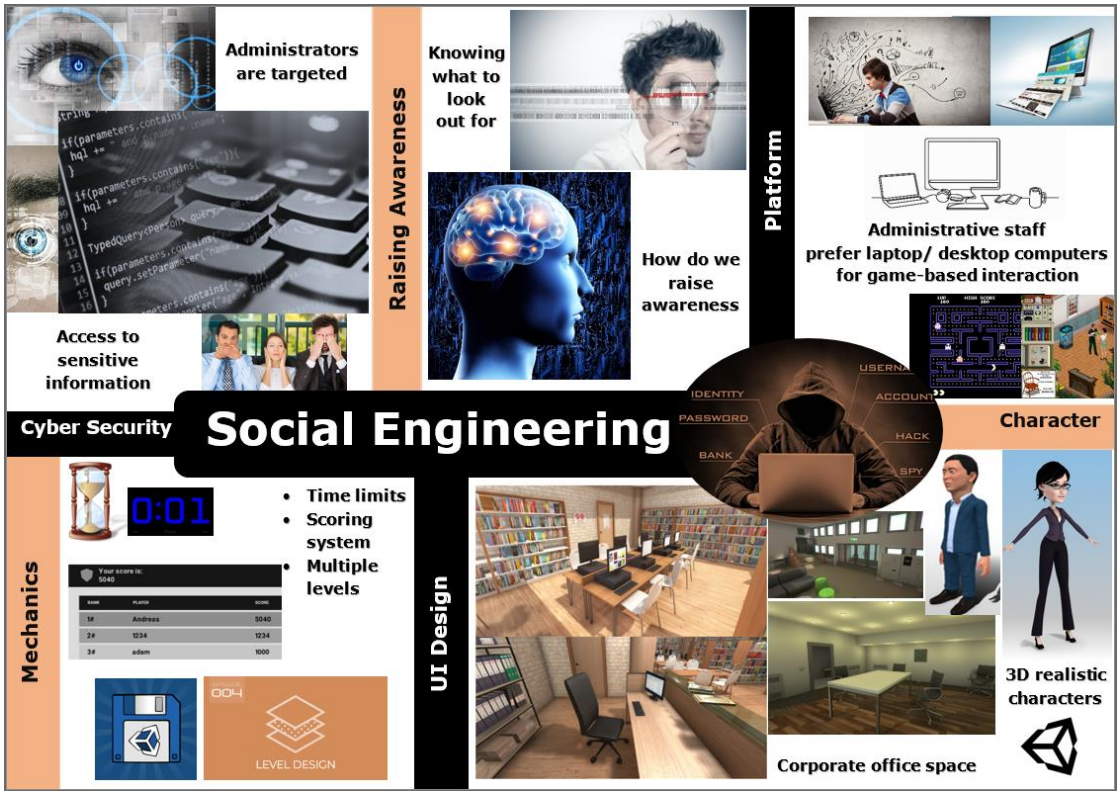


Figure 5-4: Revised conceptual mood board design (mood board 2)

5.3.1.4 Iteration 4 (conceptual prototype design)

Iteration 4 yields a conceptual prototype. The second mood board that was developed in iteration 3 is presented along with the conceptual prototype to the participants (in the second workshop). The conceptual prototype design is a translation of the confirmed design requirements, which

were depicted in mood board 2. Table 5-5 depicts the agile process that was followed for iteration 4.

Table 5-5: Iteration 4: Conceptual prototype design process

Cycle		Activity
Problem		The problem identified in this iteration was to develop a conceptual prototype that is a translation of the mood board 2 design elements. Both conceptual artefacts needed to be presented to target user group participants to confirm whether it represented the design requirements identified in workshop 1.
Design	Plan	Planning for the development of the conceptual prototype was as follows: • Obtain an understanding from internet research and design experts on how to develop a conceptual prototype (in the form of a storyboard); • Develop a conceptual prototype; and • Confirm with the participants whether the conceptual prototype and mood board are an adequate representation of the design requirements gathered from them during workshop 1.
	Requirements	Twine (version 1.4.2) can be used as a conceptual prototype development platform, and was utilised to build the storyboard (conceptual prototype).
	Design	Translating the design elements identified in the mood boards to elements that fit the conceptual prototype design requirements.
	Build	Build the conceptual prototype (refer to Figure 5-5 to Figure 5-9).
	Test	Testing is performed by confirming with the design experts from academia that the conceptual prototype adequately represents the design elements that were portrayed in the mood board 2 design.
Evaluate		The same participants who provided design requirements during workshop 1 did the evaluation of the mood board and conceptual prototype during workshop 2. Feedback was obtained regarding whether the conceptual artefacts represented the design requirements that were highlighted during workshop 1. The feedback was open-coded to identify themes in the data. These themes included suggested updates for the type of platform, the game mechanics, and the user interface design. Detailed codes can be found in Appendix G.
Revise		No. Revision of the mood board and conceptual prototype was not necessary, as it was confirmed by the participants that the artefacts adequately reflected their initial design requirements. The development process can now continue to the prototype 1 development cycle (as depicted in Figure 5-1), where the suggested updates can be implemented.

Figure 5-5 to Figure 5-9 depict screenshots from the conceptual prototype that was presented to participants during workshop 2. Figure 5-5 depicts a representation of the start-up menu, Figure 5-6 depicts a representation of the in-game corporate environment, and Figure 5-7 depicts an example of a social engineering challenge that could be presented to the user while interacting with elements in the environment. Figure 5-8 depicts an example of the learning that takes place

through related social engineering questions posed to the user, and Figure 5-9 depicts a representation of menu options available.

Figure 5-5: UI Design – start-up menu

Figure 5-6: Mechanics – in-game environment

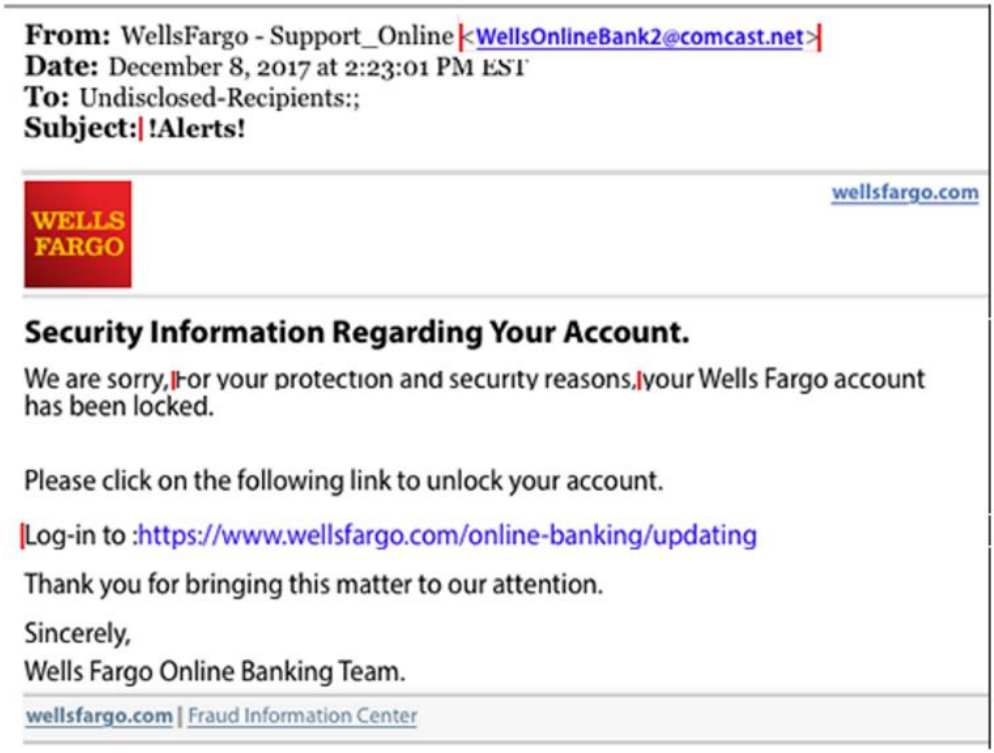


Figure 5-7: Mechanics – social engineering awareness challenge

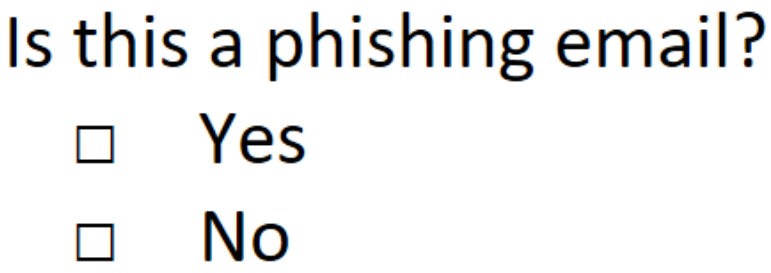


Figure 5-8: Mechanics – social engineering awareness question

Figure 5-9: UI Design – menu options

5.3.2 Artefact evaluation

Given that the design of the artefact is still in the conceptual phase of the development, it cannot be physically given to the participants to interact with for testing. Therefore, only a visual and conceptual representation of the design is presented. During the visual representation, a set of questions relevant to the design are verbally presented for discussion with the participants during the participatory design workshops. The responses to the questions are captured and analysed using open-coding, as depicted in Appendix E, and contextualised as part of the requirements gathering phase. The open-coded feedback is used as guidance to develop the prototype design, which will follow in the next chapter.

At this stage of the design, it is important to note that the evaluation of the artefact did not follow a prepared evaluation criteria, mainly because the artefact is still in a conceptual state and cannot be physically interacted with by the participants. More formalised evaluation criteria will be introduced later in this study after the development of a working prototype that the participants can interact with.

A form of evaluation of the artefact occurred verbally with the participants. The questions asked are listed in Appendix G. These questions briefly touched on the criteria defined by Mckenney and van den Akker (2005:48) as described in Chapter 4, although at this stage, they are not specifically mapped.

5.4 Rigor cycle

The rigor cycle is used to guide the design cycle. References are made to the research paradigms that grounded the design process that was followed for the artefact. References are also made to the literature to identify the concepts that the design needs to address – specifically social engineering.

5.4.1 Grounding

The conceptual design is developed based on the findings from the literature as discussed in Chapter 2 and Chapter 3. The methods and processes that guide the conceptual design of the artefacts are based on the paradigms discussed in Chapter 2 as well as the recommendations made by the experts. Chapter 3 discussed the variety of cyber-security issues that were available in the research literature.

Given that the primary objective of this research is to design an artefact that could be used to solve a problem, the design science research paradigm was deemed the suitable paradigm. The design science research methodology (DSRM) process model by Peffers *et al.* (2007:54) guides the research document. The design science research cycles from Hevner (2007:2) guide the design of the artefact, and the reporting on the artefact follows the process as described by Mckenney and van den Akker (2005:49).

The literature indicated that there are several cyber-security issues identified by researchers, with the main issue being the human element falling victim to social engineering attacks. The main issues pertaining to social engineering that computer users were most vulnerable to were discussed in Chapter 3, Section 3.2.4. These social engineering examples were the cyber-security concepts that the design would need to address.

5.4.2 Additions to knowledge base

At this stage of the research, additions to the knowledgebase are a validation of the process followed by Mckenney and van den Akker (2005:51) that has yielded a conceptual artefact. Additional contributions at this stage of the research include a conference paper on creating conceptual artefacts for games, which is titled *Creating a conceptual design for a game-based artefact* and was published in the proceedings of *EdMedia and Innovate Learning 2020 Online, Netherland, June 23-26, 2020*: URL: https://learntechlib.org/noaccesspresent/217373/.

Table 5-7 is an adaptation of the research activities as followed by Mckenney and van den Akker (2005:51). Table 5-7 describes the strategies applied as well as the iterations (referred to as circuits) in which the users (participants) and experts are involved at the different cycles and

stages of the study. The number of participants are also indicated. To explain the table by example, in the *needs and context analysis* phase, two design science research experts (DSRE) were involved in performing a review (EA) of the literature during the second contact session (circuit 2) of the *literature review* cycle. A brief description of the legend depicted in Table 5-7 is tabulated in Table 5-6.

Table 5-6: Description of the legend depicted in Table 5-7

Legend item	Description
Strategies (strategies used in the cycle)	
RE=Reaction evaluation	An evaluation that aims to determine how a participant feels about the artefact.
LE=Learning evaluation	An evaluation that aims to determine whether there is a learning experience in the participant using the artefact.
AD=Artefact development	Time spent developing the artefact by the developer.
EA=Expert appraisal	Time spent by an expert performing as assessment of a circuit component.
ME= Micro evaluation	An evaluation case at a particular circuit.
TO= Tryout	Testing of the artefact by a user.
Users (users involved in the circuit)	
AIP=Academic institution participants	Participants from an academic institution who provide design inputs.
CIP=Corporate institution participants	Participants from a corporate institution who provide design inputs.
Experts (experts involved in the circuit)	
DSRE=Design science research experts	Design science research experts (from academia) who provide expert feedback at a particular circuit.
DA=Design artist	A design artist who provides expert feedback on the design elements at a particular circuit.
CSE=Cyber security expert	A cyber security expert who provides expert feedback on cyber security issues at a particular circuit.

Table 5-7: Overview of the strategies used over two cycles consisting of fourteen circuits until the completion of the artefact conceptual design

Phase	Cycle	Circuit	Strategy						Participants					#
									Users		Experts			
			AD	*EA*	*ME*	*TO*	*RE*	*LE*	*AIP*	*CIP*	*DSRE*	*DA*	*CSE*	
Needs and context analysis	*Literature review*	1												1
		2												2
		3												2
		4												2
		5												2

		6												2
		7												2
		8												1
		9												2
	Conceptual design & concept validation	10												2
		11												6
		12												3
		13												3
		14												6
Design, development and formative evaluation of prototypes	*Prototype 1*	15												-
		16												-
		17												-
	Prototype 2	18												-
		19												-
summative evaluation & testing	*Final evaluation*	20												-
	Query	21												-
	Quality review	22												-
Totals:			**5**	**8**	**4**	**3**	**0**	**0**	**2**	**0**	**13**	**2**	**1**	**38**
Estimated total participants (at this stage) when corrected for those who participated more than once:														**8**

Legend: =Strategies used = Types of participants

Strategies: AD=Artefact Development; EA=Expert Appraisal; ME=Micro Evaluation; TO=Tryout; RE=Reaction Evaluation; LE=Learning Evaluation
Users: AIP=Academic Institution Participants; CIP=Corporate Institution Participants
Experts: DSRE=Design Science Research Experts; DA=Design Artist; CSE=Cyber Security Expert

5.5 Conclusion

Table 5-8 outlined how the process for obtaining the requirements for creating the initial conceptual design was followed in this chapter (as outlined in the introduction of this chapter). This process was followed more than once as the conceptual artefact developed was improved through multiple iterations (cycles) where, in each iteration, an improvement of the artefact was performed. Figure 5-1 provided a high-level overview of the iterative approach that was followed, and Table 5-7 provided an overview of the groups of people involved in the conceptual design process. Figure 5-2 and Table 5-1 provided a summarised view of all the iterations that were followed in the conceptual design as well as the iterations that will be followed in the subsequent prototype design and summative and testing chapters (Chapters 5 to 7). This excessive information was intentionally presented early in the study to provide context to the sections that

follow as they may become challenging to follow. The conceptual design process was discussed in detail in Section 5.3.1.

Table 5-8: An outline of how the process for creating the conceptual design was followed

Step	Step description	Approach followed in the step
1	Obtain ethical clearance from the institution	Ethical clearance was obtained from the institution to perform the research with the participants. This was achieved by submitting an ethical clearance application, which was approved and an ethics number was provided by the institution. The ethics clearance certificate is attached in Appendix B.
2	Identify the target audience	The identified target audience is administrators from a medium to large organisation. Administrative staff from an academic institution (Company A) were selected to participate in the conceptual design. An email communication was sent to the participants requesting their participation. Information, such as the workshop date and its purpose, was communicated. The list of participants who were relevant to the participatory design workshops in this chapter is depicted in Appendix D.
3	Obtain their consent to be participants in the study	Consent forms were drafted. During the first workshop, the consent forms were provided to the participants for signing. The forms were explained to provide context of the detail before the participants signed. An example of the consent form can be found in Appendix C.
4	Introduce them to the study and the literature findings	A PowerPoint slideshow was presented to the participants explaining the findings from literature and the purpose of the study. The findings pertained specifically to cyber-security issues with a key focus on social engineering. The need for performing the research was also explained, including the need for developing an artefact that can help answer the problem statement. Similar available artefacts that could be used as examples to address the problem statement were also presented. An explanation of why this study would be unique was also contextualised. The literature findings that were presented in the workshops were described in Chapters 2 and 3.
5	Obtain feedback on a suitable platform for presenting an artefact of this nature	After presenting the results from literature regarding the available artefacts that can be used as an example to answer the problem statement, feedback was obtained from the participants to determine a suitable platform to present an artefact that addresses the requirements of the target participants. It was highlighted that the game-based artefact should be accessible on a desktop computer and should follow a storyboard approach.
6	Obtain feedback on the design elements pertinent to the conceptual design of the game (during workshop 1)	Two workshops were performed with the participants to obtain the conceptual design elements. In the first workshop, the initial design elements were obtained from the participants in order to develop a mood board and conceptual artefact that represents the design requirements. In order to facilitate participation, different design element questions were presented to the participants to get their design feedback. In the second workshop, the mood board and conceptual artefact were presented to participants to obtain confirmation whether the design elements were adequately captured from the initial workshop. Additional design elements were also obtained in the

Step	Step description	Approach followed in the step
		second workshop. The additional design elements would be used to develop prototype 1. The results gathered in the participatory workshop were analysed using open coding. The open-coded results for the platform selection of the conceptual design are depicted in Appendix E.
7	Create a conceptual design based on the feedback obtained and confirm the requirements were correctly captured and translated from workshop 1 (during workshop 2).	The design elements obtained from step 6 were grouped using open coding and were used to develop a conceptual artefact. As indicated in step 6, two conceptual artefacts were developed. Firstly, a mood board that represented the initial requirements gathered from the participants (see Sections 5.3.1.2 and 5.3.1.3 for description and illustration of the mood board design). Secondly, a conceptual prototype that is a translation of the requirements depicted in the mood board (see Section 5.3.1.4 for illustration of the conceptual prototype). A variety of tools were used to develop the mood board and conceptual design; these tools were discussed in Sections 5.3.1.2 to 5.3.1.4. The themes identified in the open coding of the results from workshop 2 where the conceptual prototype was presented are depicted in Appendix G.

This section of the study has provided the detailed description of the processes followed in the design of the conceptual design of the artefact. The sections that follow will provide a detailed description of the translation of this conceptual design into a working prototype that will follow multiple iterations (cycles) in its development before undergoing a final summative evaluation and test.

For the sections that follow, the most suitable game development engine will be identified that will satisfy the design requirements of the game as identified in the conceptual design process. The accompanying game assets will also need to be determined and included in the design process. At this point in the design, the game engines were carefully considered. Twine was selected as the preferred game-based artefact development platform. This selection was based on the design requirements gathered from the participants during the workshops and concept validation. It is noted that the participants preferred the storyline type of artefact, which made Twine 1.4.2 the preferred platform for developing the artefact. Provided the skills of the researcher, Unity is a preferred engine for rapidly developing the user interface (UI) for the game. It is therefore decided that Twine would be used to represent the game-play functionality and Unity engine would be used to design the game user interface (UI).

The conceptual artefact design and development process was discussed in this chapter. Prototypes 1 and 2 are developed and documented in Chapter 6. Chapter 7 documents the summative evaluation and testing of prototype 2, which evaluates the ***reaction*** and ***learning*** evaluation of the artefact, as well as the *quality* criteria of the artefact. Prototype 2 is accepted as the final working prototype for this study.

CHAPTER 6: MID-ARTEFACT [PROTOTYPE 1 & PROTOTYPE 2]

6.1 Introduction

The primary objective of this study is to design and develop an artefact that can be used to raise awareness about social engineering attacks among administrative staff in medium to large organisations. This chapter will support the primary objective by describing the process that is followed in designing and developing the game-based prototype (prototype 1 and prototype 2).

This chapter follows the mid-artefact design guidelines that were outlined in Chapter 4. This chapter will therefore document the development of a first and second prototype design.

Based on the nature of the problem the artefact seeks to solve, which is to improve (or secure) the social engineering awareness of users, the game-based prototype is titled ‘SOCIOS3C’. The first prototype design is based on the design specifications extracted from the conceptual design. The conceptual design was developed from the requirements gathered from the target participants in participatory design workshops (as described in Chapter 5). The first prototype is iteratively improved with the design experts. Once the design has reached a usable state, it is presented to a group of participants (from Company B) in a participatory design workshop for feedback. The second prototype is iteratively developed using the feedback obtained from the presentation of prototype 1 to the participants in the participatory design workshop as well as the expert feedback received from the design experts (from academia). It is important to note that the participants involved in the prototype 1 participatory design workshop (workshop 3 - which is referred to as iteration 7) are participants who fall within the target user group demographic as well as cyber security professionals, who are all from a medium to large organisation (Company B). These participants used in the third participatory design workshop are different individuals from the participants who were used in the development of the conceptual prototype (all conceptual prototype participants are from Company A). The participant details are outlined in Appendix D.

The process for developing prototype 1 and prototype 2 is summarised as follows (approach described in Chapter 4):

1. Develop the working prototype from the conceptual design prototype (conceptual prototype design was discussed in Chapter 5);

2. Obtain expert feedback and improve the prototype 1 design (over three iterations);

3. Present prototype 1 to participants for feedback in a participatory design workshop (workshop 3);

4. Develop prototype 2 based on the design feedback obtained from the participants;

5. Obtain expert feedback and improve the prototype 2 design (over two revisions); and

6. Conclude the artefact design and development, and continue to the artefact summative evaluation and testing phase (in Chapter 7).

These steps form part of the first and second prototype design and are addressed in this chapter according to the DSR cycles by Hevner (2007:2), which are mainly composed of the *relevance* cycle, the *design* cycle, and the *rigor* cycle. The *relevance* cycle describes the relevance for designing the artefact and describes the requirements for building the prototype and the testing thereof. The *design* cycle describes the process for developing the artefact. A formalised evaluation (a mini evaluation as described in Chapter 4) of the artefact occurs with a set of participants in a participatory design workshop where the participants are allowed to interact with the artefact and provide feedback on the artefact. It is important to note that a summative evaluation and test of the artefact, to determine whether it brought about a learning experience and how participants feel about the learning experience, is performed in Chapter 7 and is not the evaluation that occurs at this stage. The summative evaluation and testing will be performed according to two levels of the four-level model for evaluating educational artefacts, by Petri and von Wangenheim (2016:995). The *rigor* cycle describes the grounding that guides the development of the artefact. The rigor cycle also takes note of any contributions that can be made to the research knowledge base.

6.2 Overview of social engineering concepts built into the game-based prototype

Ten social engineering attack types were identified and discussed in Section 3.2.4. The social engineering attack types were phishing, pretexting, baiting, quid pro quo, tailgating, dumpster diving, shoulder surfing, advanced persistent threat (APT), reverse social engineering, and water-holing. Based on the literature reviews conducted, six of these attack types were incorporated into the game-based artefact. These six types are not necessarily the most important social engineering concerns, but rather represent a balanced combination of attacks that are applicable in the relevant environments. Table 6-1 provides a description of the six attack types and how they are planned on being presented in the artefact.

Table 6-1: A description of the six social engineering attack types and their planned implementation

Attack type	Description	Presentation in the game-based artefact
Phishing	Phishing attacks occur when users click on links that redirect them to legitimate looking but malicious websites that use fear tactics to scare users to divulge sensitive information.	Phishing will be represented as an email with multiple cues for the player to determine whether it represents a social engineering attack. The player will then be asked if the email looks suspicious; if it does, the player is asked through a yes/no questionnaire whether the attack is a social engineering attack. Should the user get the question wrong, a video will play, which explains phishing and how it can be identified. The video will provide the learning experience about phishing.
Baiting	This attack is similar to that of a phishing attack, except that it lures victims into divulging sensitive information by promising them something if they provide the information.	The player will collect a USB flash drive and will be given an option to plug the USB flash drive into the computer to see what is on it. Plugging in the USB flash drive will display multiple files the user can click, one of which contains a virus. When the user clicks the virus, a video will play explaining baiting attacks. The video will provide the learning experience about baiting.
Tailgating	This type of attack occurs when the attacker gains physical access to a restricted area by impersonating a trusted entity to the victims.	The player will be presented with a scenario that gives them a choice to enter a restricted area. Entering the restricted area will provide the player with an explanation of tailgating. The learning experience will occur through the player reading the explanation on tailgating.
Dumpster diving	Dumpster diving, otherwise known as trashing, is a social engineering technique that is focused on an organisation's trash in order to possibly obtain sensitive information that is contained in documents that have been thrown away without being shredded.	The player will be presented with a problem of identifying who the receptionist in the library is. The player will be able to click on the trash bin to search for any paperwork that can provide this information. The player will find a password of the administrator instead. The player will then be presented with a yes/no question to decide whether they participated in a malicious act. Choosing the incorrect option will result in a video playing, which explains dumpster diving. A video will provide the learning experience on dumpster diving attacks.
Shoulder surfing	Shoulder surfing is a technique that is used to gather sensitive information by essentially looking over the victim's shoulder to obtain sensitive information.	Once the player has used the tailgating attack (discussed in this table) to get access to the restricted area, a shoulder surfing attack will be presented to the player. The learning experience will occur through the player seeing a username and password over an in-game character's shoulder and an explanation of shoulder surfing being displayed to the player. The learning experience will occur by showing and informing the player what shoulder surfing is.
Waterholing & phishing	It is a social engineering attack that requires a legitimate website (often used by the victim) to be compromised and used to obtain sensitive information from the target victim.	The waterholing and phishing attacks will occur in the same scene. The reason for this is that waterholing attacks are commonly coupled with rogue access points that trick users to connect to them. This will then present the user with a login screen that can be used to siphon the user's credentials. The user clicking the *Login* button on the Wi-Fi login page will trigger the event that the player has fallen victim to phishing attack. The learning

Attack type	Description	Presentation in the game-based artefact
		experience will occur through an audio cue that explains phishing attacks and a video that will explain waterholing attacks.

Throughout this chapter, screenshots of the game-based artefact during its development are presented. A final summary of the visual design will be provided in Chapter 7, along with a link to access the game-based artefact.

6.3 Relevance cycle

The *requirements* necessary for building the prototype design are translated from the conceptual design created in Chapter 5, as well as the feedback received from the participants and design experts. The key criteria that will be used to *test* the design follow from Section 4.2.2 in Chapter 4.

6.3.1 Requirements

The requirements for building this first prototype are translated from the requirements that were gathered in the conceptual design. The prototype seeks to develop a working product from the conceptual design. The second prototype development is an improvement of the first prototype design, where the lessons learnt from prototype 1 are incorporated into prototype 2.

The tools used to develop the first prototype are an extension of the tools used to develop the conceptual prototype. The additional tools that are incorporated, apart from the Twine game engine for storyboarding and the Unity game engine for the user interface development, are: Image Map, NaturalReader, Microsoft Azure, Blender, Microsoft Internet Information Service (IIS) as well as the Hyper-Text Mark-up Language (HTML) and JavaScript programming languages. Image map is an online tool that allows you to create clickable areas (also known as heat maps) on images that are embedded on web pages. NaturalReader is a text-to-speech conversion tool that is used to create voice-overs and cue explanations during the game-play. Microsoft Azure is a cloud computing service provider that is used to host the prototype and allows it to be accessed over the Internet. Blender is a tool that can be used to create 3D models that can be used in Unity as assets. HTML and JavaScript are web programming languages that are used for application functionality purposes.

The tools used to develop the second prototype are similar to those used in prototype 1, with the addition of LetsEncrypt as a certificate authority for the end-to-end data encryption on the artefact. Apache web server is substituted in the place of Microsoft IIS, and Cloudflare is introduced as the

Distributed Denial of Service (DDoS) mitigation and web application firewall (WAF) service. GoDaddy is also used as the domain registrar for the artefact.

6.3.2 Testing

During the initial development of the prototype, testing is performed by the experts (from academia) who determine whether the prototype is designed in a way that would be suitable to meet the requirements that were gathered in Chapter 5. The testing with the experts in academia occurs over two cycles, and feedback on improving the design is provided to the researcher. Once a suitable prototype is developed, it is presented to the participants to interact with for evaluation and feedback. The development and testing of prototype 1 occurs over three iterations (iteration 5 to7) with the research experts. The development and testing of prototype 2 occurs over two iterations (iterations 8 and 9). Refer to *Test* section in the Tables defined at Section 6.4.1 which describe the test results at each iteration.

6.4 Design cycle

The design of the artefact follows a similar approach as that of the Mckenney and van den Akker (2005:48) and the Heymann and Greeff (2018:498) studies. This *design* cycle aims to develop a prototype artefact. Figure 6-1 provides a summarised view of the cyclical approach that is followed in the development of the prototype artefact. Two prototype development cycles are performed, where the first prototype development cycle is a translation of the conceptual prototype (developed in Chapter 5), and the second prototype development cycle is an improvement of the first prototype. In the development of the first prototype, two iterations (iterations 5 and 6) of the design feedback are received from the design experts. The prototype is then presented to a group of participants (iteration 7), who provide design feedback. The feedback received from the participants is used to develop the second prototype, which also undergoes two development iterations (iterations 8 and 9). The development of the first and second prototype is mostly guided by the inputs received from the design experts (from academia). This iterative development process for building prototype 1 and prototype 2 is discussed in detail in Sections 6.4.1.1 to 6.4.1.5. A detailed summary of the participant involvement in each cycle as well as the events that occurred at each circuit (iteration) is depicted in Table 6-11 of Section 6.5.2.

Figure 6-1 depicts the *phases*, the *cycles* that occur at each phase, as well as the *number of participants* who are involved in each cycle for the development of the respective prototypes. In each of the artefact design and development cycles, an iterative approach is followed that requires that the artefact *problem* be identified, that the *design* is developed through a technical approach that involves *planning*, gathering the *requirements* for the artefact, *designing* it, *building* it, then

finally *testing* it. Testing will determine whether the process will be repeated from the planning step or whether the process can continue to the *evaluation* of the artefact. A decision can then be made whether the *problem* step should be started again or whether the cycle can *stop*. This approach is similar to an agile development methodology, in that it strongly involves the end users and developers throughout the development process (Cordeiro *et al.*, 2007:197).

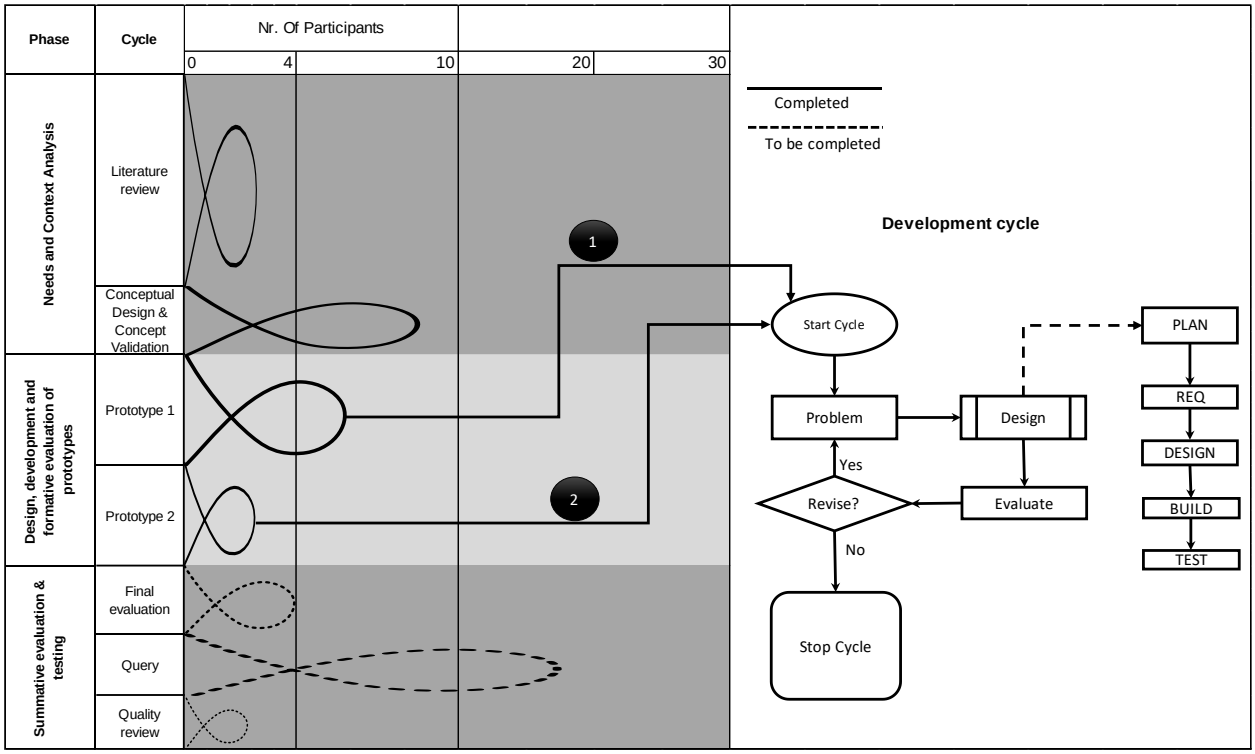


Figure 6-1: Research cycle for the prototype (prototype 1 & 2) design of the artefact

The prototype 1 cycle consists of two development iterations (iterations 5 and 6). The iterations are a continuation of those discussed in Chapter 5. *Iteration 5* (Section 6.4.1.1) is the initial development of the prototype, and *iteration 6* (Section 6.4.1.2) is the improvement of that prototype.

Iteration 7 (Section 6.4.1.3) is workshop 3, which is a participatory design workshop to evaluate the game-based artefact, as well as gathering additional design requirements.

Similar to the process followed in the development of prototype 1, the prototype 2 cycle also consists of two development iterations (*iteration 8* and *iteration 9*). The iterations are a continuation of prototype 1. *Iteration 8* (Section 6.4.1.4) is the initial development of prototype 2, and *iteration 9* (Section 6.4.1.5) is the improvement of that prototype.

The section that follows will document the iterative process that is followed in designing the prototype 1 and 2 game-based artefact, as well as the testing thereof. Chapter 7 will discuss the summative evaluation and testing of prototype 2 as a final artefact for this research study (as was described in Chapter 4, Section 4.2.2.1).

6.4.1 Artefact design

This section will discuss the prototype 1 and prototype 2 design and development processes. It is important that Figure 5-2 and Table 5-1 in Chapter 5 are referred to before reading through this section as the table and figure will provide clarity on the iterations and revisions followed in the development of prototype 1 and prototype 2. An overview is provided on the five iterations that form part of this phase of developing the working prototype (prototype 2). The objectives of these iterations are to develop prototype 1 (iterations 5 and 6), to present prototype 1 to a group of participants in a participatory design workshop (iteration 7), and to demonstrate the design and development of prototype 2 (iterations 8 and 9).

Iteration 7 includes a participatory workshop that allows prototype 1 to be presented to the participants in order to obtain feedback on the artefact's design as well as to obtain additional design requirements that are suitable for the target audience. Iterations 5 and 6 as well as 8 and 9 are designed using design expert feedback. It is important to note that the section that follows refers to the development of prototype 1 taking place over three iterations, which have two revisions (revisions 1 and 2). The same applies for the prototype 2 development terminology, which has also two revisions, i.e. revisions 1 and 2.

This section of the prototype development is best read after reviewing Figure 5-2 and Table 5-1, and with an understanding of Figure 6-1, while using Table 6-11 (in Section 6.5.2) for context of the people and activities involved at each circuit (iteration) of the prototype development cycle. It is also important to note that two design experts (from academia) were involved throughout the prototype development process.

6.4.1.1 Iteration 5 (prototype 1 development and expert feedback)

In iteration 5, the first prototype is developed. The results from the conceptual design (developed in Chapter 5) are developed into a prototype that is presented to the design experts from academia. Figure 6-2 to Figure 6-4 depict screenshots from the first revision of the prototype 1 design. Table 6-2 depicts the process that is followed for this iteration, and Table 6-3 the results from the design experts' feedback.

Table 6-2: Iteration 5 – first prototype development (no revision)

Cycle		Activity
Problem		The problem identified in this iteration is to determine how the design requirements depicted in the conceptual design can be translated into a working prototype. The purpose of translating these conceptual requirements into a prototype is to allow the design experts to evaluate the design and to provide feedback on possible improvements.

Design	Plan	Planning for the development of the first prototype required the following action items to be performed in this iteration:
		• Identify the resources, such as the user interface (UI) resources, programming languages and tools that would be used to build the prototype, such as:
		  ○ the Twine version 1.4.2 storyboarding engine, which can be used to develop the prototype functionality;
		  ○ the Unity version 2019.1.14 game engine, which can be used to create the user interface design;
		  ○ Blender, which can be used to develop 3D models that can be used as assets in Unity;
		  ○ the Hyper-Text Mark-up Language (HMTL) and JavaScript programming language, which can be used to develop the additional functionality requirements that Twine is not able to provide, such as the creation of heat maps on images, and displaying alerts on the web browser;
		• Build the prototype artefact using resources that cater for the requirements depicted in the conceptual design; and
		• Present the prototype to the design experts for feedback.

	Requirements	The requirements for the prototype were gathered from the participants in the participatory design sessions (full requirements depicted in the conceptual prototype), the design experts (from academia), as well as the literature review. The required features for the game were: • the user interface should be simplified; • the game should be playable on a desktop computer or laptop, which would enable the game to be playable on a standard web browser without requiring any installation of software on the user's machine. This would allow the game to be played on the user's work computer; • the game should not take a lot of time to play; • the concepts that are embedded into the game through play should also be explained via video; • the user should have a clearly defined avatar that represents their real-world role in the game; • the game should contain areas that speak to the social engineering concepts chosen from the literature, which are depicted in Section 6.2; • the game should not only be presented with yes/no questions; • the game should keep a point scoring system to allow the user to track their progress; • the game should allow the player to save their progress for later play; and

		• the game should have in-game instructions explaining what the player should do next.
	Design	The following tools and activities were required to build the first prototype (as revision one) and obtain design feedback (at the *test* phase) from the design experts: • To obtain a better understanding of the game design platforms (the Twine and Unity engines) that will be used to build the artefact functionality and user interface; • To obtain an understanding of using Blender, which would be used to create or modify assets in that could not be obtained from the Unity Asset Store; • To obtain the resources that will be used on the game design platform, which align to the design requirements; • To modify the resources where necessary to align with the design requirements; and • To draft a design based on the requirements, by laying out the logical flow of processes and scenes on a piece of paper before development.
	Build	The following items were built for evaluation by the design experts: • Build the prototype artefact functionality in Twine; and • Design the user interface (UI) for the Twine prototype using Unity and Blender as the game asset modelling tool. Figure 6-2 to Figure 6-4 depict examples of the artefact build results.
	Test	The following design testing was performed with the design experts: • Confirmation that the prototype adequately represents the design requirements depicted in the conceptual design; and • Confirmation that the design elements are adequate and whether additional design requirements are needed. The expert feedback obtained from the design experts is provided in detail in Appendix H. These issues identified by the design experts are summarised in Table 6-3.
Evaluate		Evaluation of the prototype was not applicable yet, as the development of prototype 1 was incomplete.
Revise		Yes. According to the design experts, the prototype needed improvement. The development of prototype 1 can be continued as iteration 6 (revision 1) and should incorporate the expert design feedback (from the artefact *testing*).

Figure 6-2 is an example of the start screen menu when starting the gameplay. It allows the game to be started or quit. It also allows the options menu to be accessed. Figure 6-3 depicts the gameplay when the game is started and the character is spawned. The design of the character environment translates to the participant design requirements, which indicated that the environment should depict that of an academic institute and a corporate institute. Figure 6-4 depicts an example of the learning that takes place through related social engineering challenges posed to the user. The challenge here is for the user to decide to either click (or choose from the available options in this version of the prototype) on the malicious files or not. If the user decides

to click on a file, it would resemble a baiting attack. The user is also given an option to cancel and not click on any of the files.

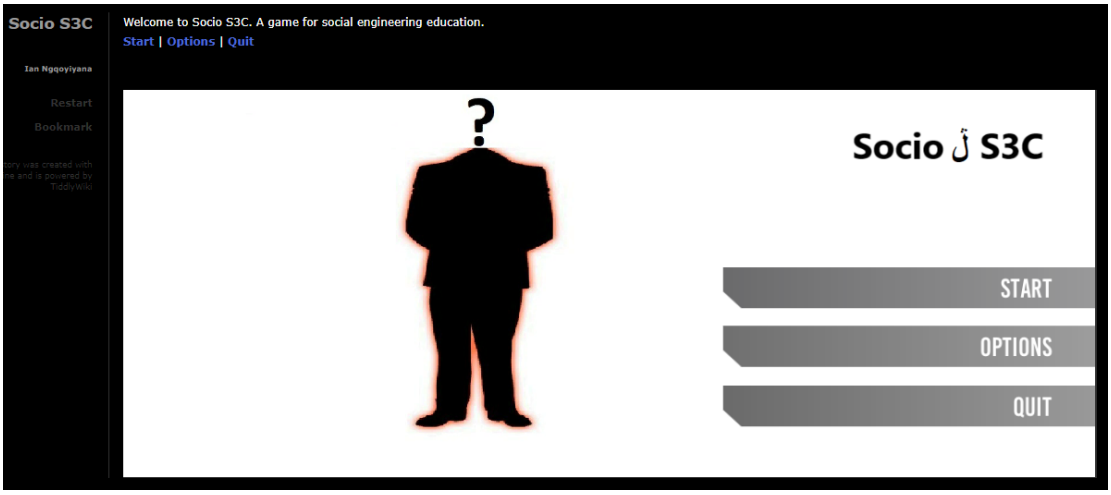


Figure 6-2: UI design – start menu

Figure 6-3: Mechanics – game start

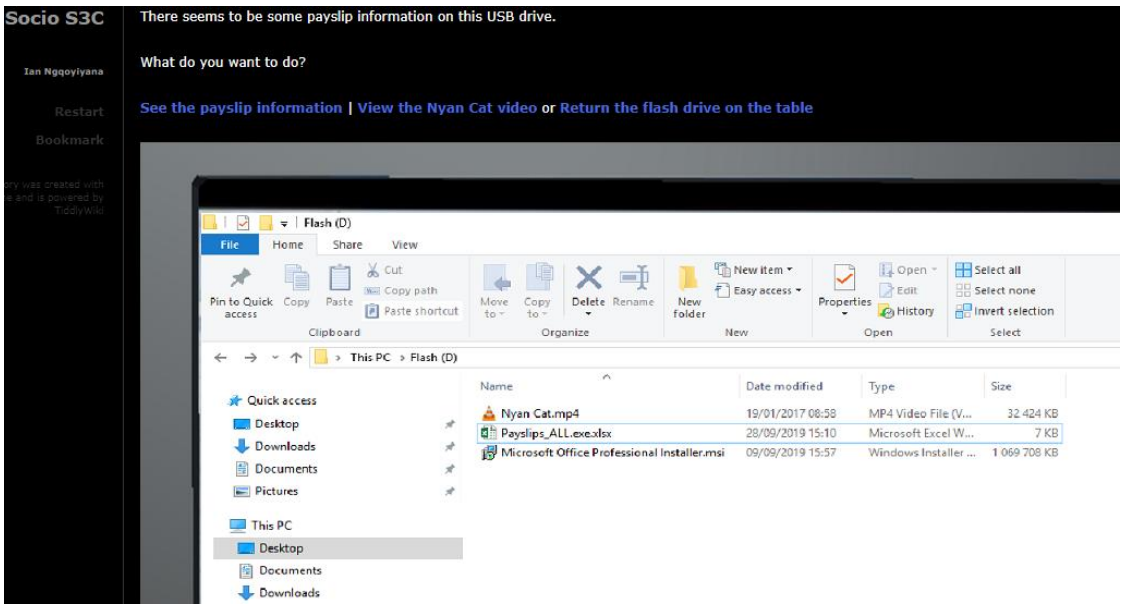


Figure 6-4: Mechanics – social engineering awareness challenge – baiting

The prototype artefact is developed (as per examples depicted in Figures 6-2 to 6-4) and presented to the design experts from academia and multiple feedback points are raised. Table 6-3 depicts a summary of these points. The full description of these points with supporting images for the feedback received for this iteration is provided in Appendix H.

Table 6-3: Summary of design issues identified by design experts during iteration 5

Design issue	Design expert response
Unsafe landing page	The landing page of the game does not have a valid certificate and therefore provides the user with a certificate error.
Dark start screen	The screen is too dark.
Game title is misaligned	The name of the game should be placed on the large black space on the top right part of the screen.
Misalignment of the player name and email text boxes	The two text boxes that capture the player's name and email address should be aligned at the right of the screen.
Un-interactive start screen	The buttons on the start screen image should be made clickable. Image map can be used to achieve this design requirement.
Inconsistent button styling on start screen	The button styles are inconsistent to those of the start screen buttons.
Inconsistent character design on the character select screen	The characters are not demonstrating consistent design, specifically around the dress code.
Inconsistent design on the introduction screen	The character selection button does not change the character when playing the actual game.

Design issue	Design expert response
	The text in the game is switching between lowercase and uppercase. The game-menu text styling is not consistent with that of the start menus.
Incorrect button positioning on the facility screen	The action buttons are not on the correct side, i.e. the left-hand option and the right-hand option should be switched around.
Missing in-game menu at the library scene	There is no menu screen at the library scene.
There is no indication of where the player is located	The player has no context where they are. A form of feedback should be provided that indicates the player's location.
The library entrance does not reflect its importance	The library entrance should be more ornate.
Unnecessary screen at the *read email on computer screen* scene	The email reader screen serves no purpose and should rather allow a user to go straight into the email, or alternatively have a couple of emails that can be clicked.
No autonomy implemented on the *read email* screen	No autonomy is implemented at the read email screen. The screen should present more autonomy by providing more than just yes/no questions to the player.
Un-interactive plug in flash drive screen	There should be more interactive functionality for the plug in flash drive scene. The scene should allow a user to click and visually experience the interaction.

The design issues listed in Table 6-3 (full list in Appendix H) are incorporated into the prototype, and the improved prototype (as revision two) is presented to the design experts. The experts provide additional feedback as part of iteration 6.

6.4.1.2 Iteration 6 (prototype 1 improvement and expert feedback)

In iteration 6, the initial prototype (from iteration 5) is improved using the design experts' feedback. Table 6-4 depicts the process that is followed for this iteration and Table 6-5 a summary of the design experts' feedback.

Table 6-4: Iteration 6 – first prototype development (revision 1)

Cycle		Activity
Problem		The problem identified in this iteration is to revise the first prototype with guidance from the design experts (from academia). The revised prototype needs to be presented to the design experts for testing and expert design feedback. The design experts will determine whether another revision is necessary for the prototype development or whether the artefact can be presented to participants.
Design	Plan	Planning for the revision of prototype 1 is as follows:

		• Obtain the appropriate design elements that reflect the changes required by the experts at the *testing* phase of iteration 5;
		• Develop an improved prototype using the appropriate tools and identified design elements such as:
		  ○ Twine version 1.4.2, which can be used to develop the functionality of the prototype;
		  ○ Unity version 2019.1.14, which can be used to design the user interface;
		  ○ Blender, which can be used to develop models that are not available on the Unity asset store;
		  ○ Microsoft Internet Information Services 8.0 (IIS), which can be used as the web server to host the application. The web server can be deployed in Microsoft Azure, which is a cloud computing service provider that can allow the game-based artefact to be hosted online so that it can be accessed from anywhere over the Internet;
		  ○ LetsEncrypt, which can be used as a trusted certificate authority (CA) for securing the network traffic using end-to-end encryption and validating the authenticity of the game-based artefact when users visit it; and
		• Obtain confirmation from the design experts that an adequate design can be presented to the participants.

	Requirements	The first revision (iteration 6) of prototype 1 is built from the base laid down in the development of prototype 1 (iteration 5). The requirements are gathered from the feedback received from the design experts during the testing in iteration 5 in order to improve the prototype. The required features (translated from Table 6-3) for the game improvement were: • the game should have a valid certificate from a trusted certificate authority; • the game's theme is too dark and should be lightened up using lighter background colours; • the text boxes that capture the player's name and email address should be aligned at the right of the screen; • the buttons on the facility scene should be repositioned to a more suitable area; • the library scene in the game should have a menu screen; • the start screen should be more interactive by providing additional options for configuring the game environment; • the game should provide the player with an indication of where they are in the game; • the screen where the player reads the email should provide more interaction points; and • the screen where the player plugs in the flash drive should provide more interaction points.
	Design	The following tools and activities were required to build the second revision of the first prototype and obtain design feedback (at the *Test* phase) from the design experts: • To obtain an understanding on how to setup and start-up a virtual machine on Microsoft Azure, as well as setting up the Firewall rules to allow the artefact to be accessed from any Internet address; • To obtain an understanding on how to implement a valid certificate from a certificate authority such as LetsEncrypt to

		secure the end-to-end network connection through the hyper-text transfer protocol (HTTPS) and to validate the authenticity of the website that is hosting the artefact; • To obtain an understanding on how to deploy the game-based artefact onto Microsoft IIS as a web server; • To obtain the updated resources that will be used on the game design platform, which align to the design requirements, such as improved character avatars; • To modify the resources where necessary using Blender to align with the design requirements; and • To draft a design based on the requirements, by laying out the logical flow of processes and scenes on a piece of paper before development.
	Build	Build the improved prototype as revision two using the requirements gathered from the design experts in revision one and incorporate additional tools identified in revision one. Figure 6-5 to Figure 6-7 depict examples of the artefact build results.
	Test	Testing is performed by confirming with the design experts from academia: • That the prototype build adequately represents the design elements that were identified during the expert feedback in the *test* phase of iteration 5; and • Whether any additional design feedback is required to improve prototype 1. A detailed description with images of the design feedback is illustrated in Appendix I. These design issues identified by the design experts are summarised in Table 6-5.
Evaluate		Evaluation of the prototype was not applicable yet, as the development of the prototype was incomplete.
Revise		Yes. According to the design experts, the prototype needed improvement. The development of prototype 1 can be continued as iteration 7 (as revision 2) and should incorporate the expert feedback (from the *testing* phase).

Figure 6-5 is an example of the start screen menu when the gameplay is started. It is the screen that allows the user to start a new game or continue from a saved game (only one game save slot can be used per player). Figure 6-6 depicts the gameplay when the game is started and the character is spawned. This screen is similar to the screen depicted in iteration 5 (as Figure 6-3), with some cosmetic improvements and the ability to choose characters. Figure 6-7 depicts an example of the learning that takes place through related social engineering scenarios. The player is given an option to enter a restricted room they should not be accessing or to go back to the lobby. If the player enters the room, an alert is triggered, warning the player of the tailgating attack that has taken place.

Figure 6-5: UI design – start menu

Figure 6-6: Mechanics – game start

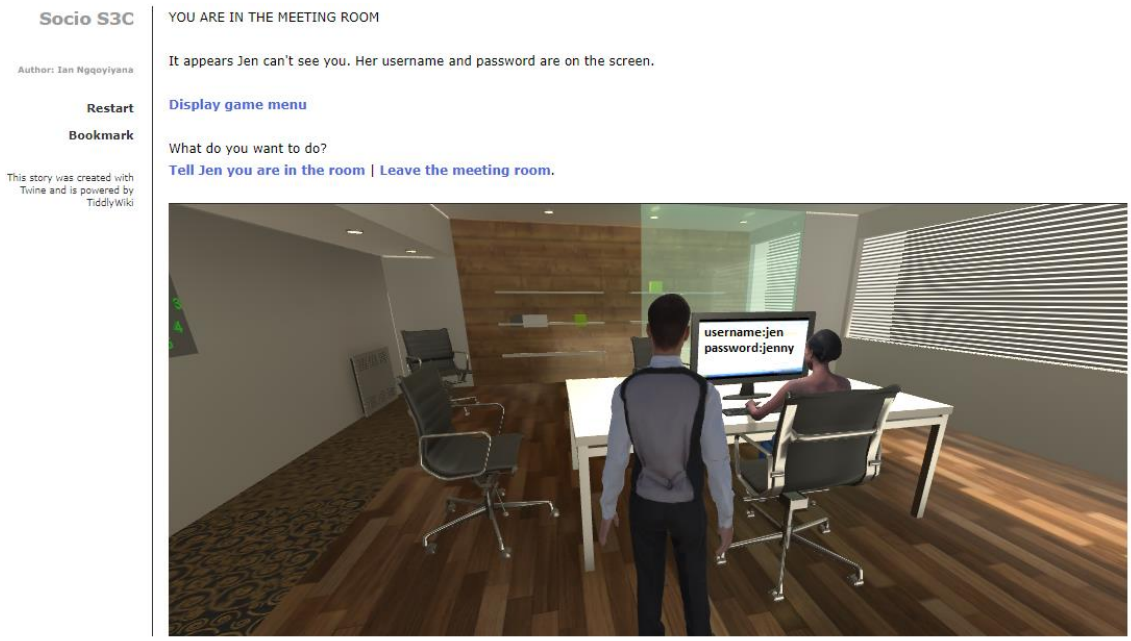


Figure 6-7: Mechanics – social engineering awareness challenge – shoulder surfing

The feedback received from the experts in iteration 6 is summarised in Table 6-5. The full description with supporting images for the feedback received is depicted in Appendix I.

Table 6-5: Summary of design issues identified by design experts during iteration 6

Issue	Design expert response
The sound mute button is not working in the options screen	The sound mute option is not working. Once clicked, it shows an alert message indicating that the sound is muted, but the sound is not actually muted.
A server error appears when clicking a button on the start screen	Clicking the *continue game* button on the game start screen presents a server error. The error should be more descriptive to the player and allow the game-play to continue.
There are inconsistent character designs when selecting a character on the new game screen	The character designs are very different from each other and need to be designed in a way that makes them more consistent by design.
There is limited interactivity of a character	The overall interactivity of the character mobility should be improved through the use of hotspots rather than text links at the top of the screen.
Inconsistent screen sizes	The main game screen size and game menu screen sizes are not equivalent and should be resized to the same dimensions.
Abrupt event on the meeting room entrance scene	The indication of the tail-gating event occurs abruptly and should be altered in a way that it is obvious and allows the user to decide whether the event should happen or not.

Issue	Design expert response
There is a loose story tail in the meeting room scene	There is a loose story tail in the meeting room scene where an audio clip plays but nothing happens.

6.4.1.3 Iteration 7 (prototype 1 improvement and workshop presentation)

In iteration 7, the improved prototype developed after incorporating the expert feedback from iteration 6 is presented to a different participant group in a third participatory design workshop. The purpose of presenting the prototype in a participatory design workshop is to obtain additional design feedback from a different participant group (participants that have not been included in the research yet) who also fall within the demographic of the target audience. It also provides confirmation whether the game-based artefact can cater for users in a different organisation to those who formed part of the initial participatory design workshops. Table 6-6 depicts the process that is followed for this iteration.

Table 6-6: Iteration 7 – first prototype development and workshop presentation (revision 2)

Cycle		Activity
Problem		The problem identified in this iteration is to revise the first prototype with feedback obtained from the design experts (from academia). The revised prototype needs to be presented in a participatory design workshop to a different set of participants to those who were involved in the conceptual prototype design. The design experts will determine whether another revision is necessary for the prototype development or whether the artefact can be presented to participants.

Design	Plan	Planning for the revision of prototype 1 is as follows:
		• Obtain the appropriate design elements that reflect the changes identified by the experts at the *test* phase of iteration 6;
		• Develop an improved prototype using the appropriate tools and the design elements identified by the experts, such as
		  ○ Twine version 1.4.2, which can be used to develop the functionality of the prototype;
		  ○ Unity version 2019.1.14, which can be used to design the user interface;
		  ○ Image map, which is a tool that can be used to convert images into clickable areas called heat maps;
		  ○ NaturalReader, which is a tool that can be used to convert text to speech for scene voice-overs such as in the game tutorial or at important cues;
		• Obtain confirmation from the design experts that an adequate design can be presented to the participants; and
		• Present the improved prototype to the participants, if applicable. When presenting the artefact for play during the participatory design workshop, it is important that all the participants have a

		computer or laptop with earphones and an active Internet connection. This will allow the participants to access the game-based artefact and have an enhanced experience when interacting with it during game-play.
	Requirements	The requirements are gathered from the feedback received from the design experts in order to improve the first prototype and apply the necessary changes. The required features (translated from Table 6-5) for the game improvement were: • the sound mute button on the options screen should be fixed; • the errors shown in the game should be more appealing to the player and allow the play to continue playing and not send them back to the start screen; • the character designs are inconsistent and should be aligned to be more consistent; • the game should have more interaction points through the use of heat maps; • the game screen sizes are not consistent; • the software bug that causes an abrupt event in the meeting room entrance scene should be fixed; and • the loose story tail in the meeting room scene should be recreated to allow continuity in the game-play story.
	Design	The following tools and activities were required to build the second revision of the first prototype and obtain design feedback (at the *test* phase) from the design experts: • To obtain the resources that will be used on the game design platform that align to the design requirements obtained from the design experts in the *test* phase of iteration 6, such as creating a more interactive design as well as displaying a user friendly error message; • To obtain a better understanding of how to use NaturalReader as the tool that can be used to create voice-overs in the game, such as the voice over that occurs during the library scene when the player approaches the receptionist's desk; • To obtain a better understanding of how to use Image Map as the tool that can be used to create heat maps on images making them clickable and thereby providing an enhanced game-play experience, such as the heat mapping implementation on the menu screens; • To modify the resources, where necessary, such as adjusting the game menu size for consistency, to align with the design requirements; and • To draft a design based on the requirements, by laying out the logical flow of processes and scenes on a piece of paper before development.
	Build	Build the improved prototype as revision three using the requirements gathered from the design experts in revision two (iteration 7).
	Test	Testing is performed by confirming with the design experts from academia: • That the prototype build adequately represents the design elements that were identified during the expert feedback in the *test* phase of iteration 6 (revision 2); and • Whether any additional design requirements should be included.

		No additional design issues are identified by the design experts and the artefact can now be evaluated by the participants. The feedback from the participants evaluating the artefact would therefore be used to improve the design.
Evaluate		The prototype has been developed to a usable and presentable state. The prototype is presented to a set of participants from a medium to large organisation. Feedback is obtained regarding whether the prototype is fit for purpose and whether it can be improved to be more suitable. The results from the evaluation are grouped into coded themes. The coded themes are depicted in Appendix J. These themes included suggestions to make the game more interactive, especially with random objects, allowing the player to walk around freely, as well as including a mechanism of notifying the player when they have completed the game. A summary of the participant feedback is tabulated as Table 6-7.
Revise		No. After consultation with the design experts and participants in workshop 3, the design cycle for prototype 1 can be concluded. The feedback obtained during iteration 7 will now roll over to the development of prototype 2.

Table 6-7: Summary of design issues identified by participants during the iteration 7 workshop

Issue	Participant response
The player is confused on what to click when the game starts	It is not clear what should be clicked when the game starts.
The objective of the game is unclear	The objective of the game is not clearly stipulated at the beginning of the game.
There is a game-play error in the meeting room scene	The game-play in the meeting room scene displays an error when attempting to enter the room.
The dumpster diving challenge is not clear	The dumpster diving challenge is not clear enough, it should be more obvious to the player that the aim is for the character to click on the trash bin.
There is an error in the meeting room scene when playing the female character	The female character triggers an error when the character walks to the passage and tries to walk back.
The game is not interactive enough	Hotspots or heat maps will work better if used in the entire game.
It is not clear when the game ends	The game should indicate when all challenges have been completed.
The tailgating scene challenge is not clear	The tailgating challenge is not clear enough and should be presented well enough for the user to identify it and have the option to correct their choice.
The game is not exploratory	The game should allow the character to walk freely around the map and should not be limited to specific moves.

The prototype artefact was improved in this second development revision and presented to the design experts and second group of participants at workshop 3. No artefact design snapshots are

captured as no requirements were gathered from design experts in this cycle. The requirements gathered in this cycle are from the participants during the third workshop that took place. The requirements were open coded to identify themes in the data and tabulated in Appendix J. These open coded themes will be used to develop prototype 2 in iteration 8.

6.4.1.4 Iteration 8 (prototype 2 development and expert feedback)

Iteration 8 is the development of prototype 2 (which is developed over iterations 8 and 9). Table 6-8 depicts the process that is followed for this iteration.

Table 6-8: Iteration 8 – second prototype development (revision 1)

Cycle		Activity
Problem		The problem identified in this iteration is to develop prototype 2 using the feedback received from the participants in workshop 3 (iteration 7) and to obtain feedback from the design experts. The design experts will determine whether the artefact requires a revision for design improvement or can be presented for the final evaluation and testing.

Design	Plan	Planning for the development of prototype 2 is as follows:
		• Obtain the appropriate design elements that reflect the changes required by the participants in workshop 3 (iteration 7) as well as any additional feedback from the design experts;
		• Identify the tools necessary for developing prototype 2 (no new tools were required for the development of the additional changes) such as
		  ○ Twine 1.4.2, which can be used to develop the functionality of the prototype;
		  ○ Unity 2019.1.14, which can be used to design the user interface;
		  ○ Image map, which is a tool that can be used to convert images into clickable areas called heat maps;
		  ○ NaturalReader, which is a tool that can be used to convert text to speech for scene voice-overs such as in the game tutorial or at important cues;
		• Develop prototype 2 using the appropriate tools and design elements identified in iteration 7; and
		• Present the prototype to design experts for feedback.

	Requirements	The second prototype was built from the base laid down in the first prototype of the game in iteration 7. The requirements for developing prototype 2 were mainly gathered from the participants during workshop 3 (iteration 7). The required features (translated from Table 6-7) for the prototype 2 development were: • the player should be provided with a tutorial on how to play the game and what to click at the start of the game; • the objective of the game should be clarified at the start of the game so that the player knows what is expected; • the error at the meeting room should be fixed; • the dumpster diving challenge should be made clearer;

		• the error in the meeting room scene when playing with the female character should be fixed; • the game should have more interactive points with random objects in the game world; • the game ending should be clarified so that the player knows when the game has been completed; and • the tailgating scene challenge should be clarified.
	Design	The following tools and activities were required to build the first revision of the second prototype and obtain design feedback (at the *test* phase) from the design experts: • To obtain the appropriate design elements that reflect the changes required by the participants in workshop 3 (iteration 7) • To identify any additional design requirements from the experts during the *test* phase of iteration 7; • To develop an improved prototype using the appropriate tools and design elements outlined by the participants through open coded themes during workshop 3, such as making the game more interactive using heat maps, implementing a tutorial at the beginning of the game to outline its objective, as well as developing an ending to the game storyline (see Appendix J); and • To draft a design based on the requirements, by laying out the logical flow of processes and scenes on a piece of paper before development.
	Build	Build prototype 2 using the requirements gathered in workshop 3 (iteration 7).
	Test	Testing is performed with the design experts from academia to confirm: • That prototype 2 is adequately built using the requirements gathered in workshop 3 and that it represents a suitable design; and • Whether there are additional design requirements. Given that the design is reaching a mature stage, the expert feedback is brief. The feedback mainly relates to the absence of an ending to the artefact storyline. A *feedback issues* table is therefore not created as was done for iterations 5-7. The expert feedback results are depicted in Appendix K.
Evaluate		The evaluation of the prototype was not applicable, as the development of prototype 2 was incomplete.
Revise		Yes. According to the design experts, the prototype needed improvement. The development of prototype 2 can be continued as iteration 9 (revision 2) and should incorporate the expert feedback (from the *test* phase).

The expert feedback for this iteration is not tabulated as the design of the artefact has reached a point where there is limited design feedback. The feedback relates mainly to the ending of the artefact storyline. The feedback from the design experts is provided in Appendix K and is used to develop the improvement to prototype 2 in iteration 9 (revision 2).

No artefact design snapshots (screenshots) are captured, as the requirements gathered from the design experts in this cycle were limited.

6.4.1.5 Iteration 9 (prototype 2 improvement and finalisation)

In iteration 9, the second prototype is improved based on the feedback received from the design experts. Table 6-9 depicts the process that is followed for this iteration.

Table 6-9: Iteration 9 – second prototype development (revision 2)

Cycle		Activity
Problem		The problem identified in this iteration is to improve the design of prototype 2 using the feedback received from the design experts in iteration 8 and to conclude the prototype 2 development. The final prototype should be presented to participants for summative evaluation and testing. The design experts will determine whether the artefact requires a revision for design improvement or can be presented to the final summative evaluation and testing.
Design	Plan	Planning for the development of prototype 2 is as follows: • Obtain the appropriate design elements from the *test* phase of iteration 8 that reflect the changes required by the design experts; • Identify the tools necessary for developing the improved prototype 2 such as o Twine 1.4.2, which can be used to develop the functionality of the prototype; o Unity 2019.1.14, which can be used to design the user interface; o Image map, which is a tool that can be used to convert images into clickable areas called heat maps; o NaturalReader, which is a tool that can be used to convert text to speech for scene voice-overs such as in the game tutorial or at important cues; o Apache 2.4.43 is the web server that is substituted for Microsoft Internet Information Services 8.0 (IIS). This is due to compatibility issues with Linux Ubuntu 18.04, as Linux does not support Microsoft IIS. Linux is used as the long-term application hosting operating system due to licensing fees associated with using Microsoft Windows in the cloud; o Cloudflare is used as the security layer for the web application. It provides Denial of Service (DoS) protection and web application firewall capability. It is also used for application content caching, which increases performance for content requested by users from the Apache web server; o GoDaddy is a domain registrar that is used to register the application's domain name, allowing users to request the application using an application domain name instead of an Internet protocol (IP) address; • Develop prototype 2 using the identified design improvement requirements; and • Present the prototype to the design experts for expert feedback.
	Requirements	The second revision (iteration 9) of prototype 2 is built from the base laid down in the first revision (iteration 8) of prototype 2. The requirements are gathered from the feedback received from the design experts during the

		testing in iteration 8 in order to improve the prototype. The required features (translated from Appendix K) for the game improvement were: • the game should have a clear ending; and • the game should display a scoring system at the end of the game and allow the player to revise any questions they may have gotten incorrectly. It is important to note that the tools identified in the planning are more than the items in the design requirements. This is primarily because of the migration from a Microsoft Windows virtual machine to a Linux virtual machine. The costing requirements of running a licensed Microsoft Windows virtual machine over a Linux virtual machine are higher.
	Design	The following tools and activities were required to build the second revision of the second prototype and obtain design feedback (at the *test* phase) from the design experts: • To obtain a better understanding on how to install and use Apache 2.4.43 as the application web server; • To obtain a better understanding of Cloudflare, which provides the security layer for the web application; • To obtain a better understanding of how to register and use GoDaddy as the domain name registrar; • To obtain the appropriate design elements that reflect the changes required by the experts in workshop 3 (iteration 7); • To obtain the resources that will be used on the game design platform, which align to the design requirements obtained from the design experts in the *test* phase of iteration 8, such as implementing an ending to the game play. These requirements are depicted in Appendix K; and • To draft a design based on the requirements, by laying out the logical flow of processes and scenes on a piece of paper before development.
	Build	Build the improvements to prototype 2 using the requirements identified by the design experts in the *test* phase of iteration 8.
	Test	Testing is performed with the design experts from academia to confirm: • That prototype 2 is adequately built using the requirements identified in the artefact test of iteration 8 and that the artefact represents a suitable design; and • Whether there are additional design requirements. As with iteration 8, the artefact design is reaching a mature stage, and the expert feedback is brief. The feedback mainly relates to one of the challenges not being reachable as an ending to the last challenge in the game. A feedback issue table is not created as was done for iterations 5-7. The expert feedback results are depicted in Appendix L.
Evaluate		The design experts indicate that the artefact can undergo a final evaluation to test whether it has reached the objectives set out in this study. This evaluation can be performed under condition that the issues identified during the expert testing are resolved. The prototype will be presented to participants and respondents as part of the summative evaluation and testing of the artefact. The evaluation will be performed using two of the four levels in the model by Petri and von Wangenheim (2016:995) for evaluating educational artefacts.
Revise		No. A revision is not necessary for this prototype 2 (revision 2), as the design experts indicate that the design is suitable for the final artefact summative evaluation and testing (discussed in Chapter 7).

As with iteration 8, no artefact design snapshots are captured as the design of the artefact has reached a point where there is limited design feedback. The expert feedback results are depicted in Appendix L, and were used to develop the final prototype 2 in this iteration.

6.4.2 Artefact evaluation

At this stage of the design, it is important to note that a summative evaluation and test of the artefact did not occur yet. The prototype 1 is evaluated in a participatory design feedback session which is held as workshop 3 in iteration 7.

During the workshop, the participants are given an opportunity to play the game-based artefact without any input from the researcher. The participants are asked questions similar to the questions asked in the previous participatory design workshops. The questions are asked verbally (see Appendix J for questions). The responses to the questions are captured and open-coded (also see Appendix J for open-coded responses) and then contextualised as part of an additional round of requirements gathering, which is used to develop prototype 2. These coded responses are used for guidance on how to improve the design for prototype 2.

Prototype 2 is an improvement of prototype 1. The artefact is iteratively improved using the requirements gathered from the coded themes captured in the third participatory design workshop. The design experts also provide iterative expert feedback (through testing as described in Section 6.3.2) on the improvement of the artefact until it reaches a desirable state for the summative evaluation and testing. The development of prototype 2 occurs over two iterations with the experts' feedback.

6.5 Rigor cycle

The rigor cycle is used to guide the design cycle. References are made to the research paradigms that grounded the design process that is followed for the artefact. References are also made to the literature to identify the concepts that the design needs to address – specifically social engineering.

6.5.1 Grounding

The prototype design is based on the conceptual design developed in Chapter 5. The methods and processes that guided the prototype design of the artefact are based on the knowledge and experience of the design experts from academia. Section 6.2 provides a brief discussion of the grounding on the literature (from Section 3.2.4) that guides the topics that are relevant to the

design of the artefact. These topics relate specifically to the social engineering issues identified in the literature and how the artefact aims to address them. Additional grounding criteria for the development of the prototype were discussed in the grounding discussion in Section 5.4.1 of Chapter 5.

6.5.2 Additions to knowledge base

At this stage of the research, additions to the knowledgebase are that the additional tools used worked exceptionally well. The tools include image map, which enabled interactive functionality of images and heat maps. Microsoft Azure is also an addition that enabled game resources to be hosted in the cloud and enabled them to be accessible from anywhere on the Microsoft Internet Information Service (IIS) web server as well as the Apache web server. Cloudflare is used as a Distributed Denial of Service (DDoS) mitigation and web application firewall (WAF) service. GoDaddy is also used as the domain registrar for the artefact. Table 6-11 relates particularly to Section 6.4.1, where the prototype was developed. It shows the multitude of circuits that occur in each development cycle and the users, participants and experts involved in each stage as well as the events (strategy) that took place. A brief description of the legend depicted in Table 6-11 is tabulated in Table 6-10.

Table 6-10: Description of the legend depicted in Table 6-11

Legend item	Description
Strategies (strategies used in the cycle)	
RE=Reaction evaluation	An evaluation that aims to determine how a participant feels about the artefact.
LE=Learning evaluation	An evaluation that aims to determine whether there is a learning experience in the participant using the artefact.
AD=Artefact development	Time spent developing the artefact by the developer.
EA=Expert appraisal	Time spent by an expert performing as assessment of a circuit component.
ME= Micro evaluation	An evaluation case at a particular circuit.
TO= Tryout	Testing of the artefact by a user.
Users (users involved in the circuit)	
AIP=Academic institution participants	Participants from an academic institution who provide design inputs.
CIP=Corporate institution participants	Participants from a corporate institution who provide design inputs.
Experts (experts involved in the circuit)	
DSRE=Design science research experts	Design science research experts (from academia) who provide expert feedback at a particular circuit.

Legend item	Description
DA=Design artist	A design artist who provides expert feedback on the design elements at a particular circuit.
CSE=Cyber security expert	A cyber security expert who provides expert feedback on cyber security issues at a particular circuit.

Table 6-11: Overview of the strategies used over four cycles consisting of 19 circuits until the completion of the artefact prototype 2 design

Phase	Cycle	Circuit	Strategy						Participants					#
									Users		Experts			
			AD	*EA*	*ME*	*TO*	*RE*	*LE*	*AIP*	*CIP*	*DSRE*	*DA*	*CSE*	
Needs and context analysis	*Literature review*	1		■							■			1
		2		■							■			2
		3		■							■			2
		4		■							■			2
		5		■							■			2
		6		■							■			2
		7		■							■			2
		8			■								■	1
		9		■							■			2
	Conceptual design & concept validation	10	■								■			2
		11	■			■			■		■			6
		12	■		■						■	■		3
		13	■		■	■					■	■		3
		14	■		■	■			■		■			6
Design, development and formative evaluation of prototypes	*Prototype 1*	15	■	■							■			2
		16	■	■							■			2
		17			■	■				■				4
	Prototype 2	18	■	■							■			2
		19	■	■							■			2
summative evaluation & testing	*Final evaluation*	20												-
	Query	21												-
	Quality review	22												-
Totals:			**9**	**12**	**5**	**4**	**0**	**0**	**2**	**1**	**17**	**2**	**1**	**53**
Estimated total participants when corrected for those who participated more than once:														**12**

Legend: ■ =Strategies used ■ = Types of participants

Strategies: AD=Artefact Development; EA=Expert Appraisal; ME=Micro Evaluation; TO=Tryout; RE=Reaction Evaluation; LE=Learning Evaluation;
Users: AIP=Academic Institution Participants; CIP=Corporate Institution Participants
Experts: DSRE=Design Science Research Experts; DA=Design Artist; CSE=Cyber Security Expert

6.6 Conclusion

Table 6-12 outlines how the process to obtain the requirements for creating the prototype design was followed in this chapter. This process was followed more than once as the prototype artefact developed was improved through multiple revisions over two prototype development cycles. Figure 6-1 provided an overview of the cycles that were followed in this chapter. Table 6-11 provided an overview of the circuits (iterations) that were completed up to this point of the study.

Table 6-12: An outline of how the process for creating the prototype was followed

Step	Step description	Approach followed in the step
1	Develop the working prototype from the conceptual design prototype (conceptual prototype design was discussed in Chapter 5)	The first prototype was developed from the requirements gathered in the conceptual prototype design, which was developed in Chapter 5. The first prototype was developed using mainly the Twine version 1.4.2 game development engine for the artefact functionality and Unity version 2019.1.14 for the artefact user interface design. The prototype design was improved using feedback from design experts, which occurred over two revisions (refer to test results of iteration 5 (Section 6.4.1.1) and iteration 6 (Section 6.4.1.2)). Step 2 provides a summarised explanation of the two revisions prototype 1 had undergone before being presented to the participants in workshop 3 (step 3).
2	Obtain expert feedback and improve the prototype 1 design (over two revisions)	Once a first attempt was completed of prototype 1, the prototype was presented to the design experts. The design experts provided feedback regarding the design of prototype 1. This feedback was provided over two revisions for the first prototype development process. **Prototype 1 development cycle** *Revision 1* (see Section 6.4.1.1): There were multiple issues identified by the design experts regarding the design of the artefact. The summarised expert feedback was depicted in Table 6-3 and was detailed in Appendix H. The feedback was implemented as an improvement to the prototype. *Revision 2* (see Section 6.4.1.2): This revision was the improvement of prototype 1 using the expert feedback received in revision 1. Additional feedback was also obtained regarding the design of the artefact from the experts. The feedback was summarised in Table 6-5 and detailed in Appendix I.
3	Present prototype 1 to participants for feedback in a participatory design workshop (workshop 3)	At iteration 7 (see Section 6.4.1.3), the final changes were performed on the first prototype and it was presented to a different group of participants from the participants who were involved in the prior participatory design workshops. This workshop was the third workshop that took place in the artefact development process. During the workshop, confirmation was received from the participants that the design was suitable, but needed some design improvement. The design feedback from the participants was depicted in Appendix J and was analysed using open coding to identify themes in the data.
4	Develop prototype 2 based on the design feedback obtained from the participants	Prototype 2 was developed using the feedback received from the participants in workshop 3 (step 3). As with the prototype 1 development, Twine version 1.4.2 and Unity version 2019.1.14 were used to develop prototype 2. Additional tools were also used to host the application, secure it, as well as to improve its cosmetic appearance. These additions were

Step	Step description	Approach followed in the step
		discussed over two iterations as iteration 8 (Section 6.4.1.4) and iteration 9 (Section 6.4.1.5).
5	Obtain expert feedback and improve the prototype 2 design (over two revisions)	Upon completing the first attempt of prototype 2, it was presented to the design experts for feedback, as was done for prototype 1. The expert feedback was provided over two revisions for prototype 2. **Prototype 2 development cycle** *Revision 1* (see Section 6.4.1.4): The approach was similar to that used in prototype 1, in that the prototype 2 was developed using feedback received from the participants in the participatory design workshop. The prototype was later then presented to the design experts for design feedback. The expert feedback was presented in Appendix K for revision 1. *Revision 2* (see Section 6.4.1.5): The approach was similar to that used in prototype 1 revision 2, in that prototype 2 was an improvement of revision 1 using the expert feedback. The expert feedback was depicted in Appendix L for revision 2.
6	Conclude the artefact design and development, and continue to the artefact summative evaluation and testing phase (in Chapter 7)	During testing at iteration 9 (revision 2 of prototype 2), the design experts concluded that prototype 2 had reached a suitable state and could be used to perform the final summative evaluation and testing as described in Chapter 4 (Section 4.4.2.3). The final summative evaluation and testing will be performed in Chapter 7 using two evaluation levels of the four-level model for evaluating educational artefacts by Petri and von Wangenheim (2016:995). The *quality* of the artefact will also be tested using the quality evaluation criteria by Mckenney and van den Akker (2005:48).

The prototype 2 summative evaluation and testing will occur in Chapter 7, which will determine whether the artefact has an effective design based on the ***reaction*** of the participants, as well as the ***learning*** experience of participants, and will indicate whether the artefact can be used to achieve the objectives as set out in this study. The *quality* of the artefact will also be evaluated in Chapter 7 using a set of predefined quality evaluation criteria.

CHAPTER 7: POST-ARTEFACT

7.1 Introduction

The primary objective of this study is to design and develop an artefact that can be used to raise awareness about social engineering attacks among administrative staff in medium to large organisations. This chapter will support the primary objective by describing the process that is followed in testing and evaluating the usable prototype (prototype 2) artefact, which was developed in Chapter 6.

This chapter follows the post-artefact design guidelines that were set out in Chapter 4. The goal of this chapter is to describe the summative evaluation and testing of the second prototype. The second prototype will be referred to as the game-based artefact. The game-based artefact was iteratively developed in Chapter 6 and is the final prototype for this study. It is tested and evaluated using the ***reaction*** and ***learning*** evaluation levels as described in the four-level model for artefact evaluation by Petri and von Wangenheim (2016:995). The ***reaction*** level of the artefact test is performed with participants who were involved in prior participatory design workshops during the artefact design and development stages; this level specifically aims to determine how the users who provided design input feel about the final product. The ***learning*** level is performed with a unique set of participants that were not previously involved in other areas of the study. The ***learning*** evaluation will determine whether the artefact encourages a learning experience regarding the identified social engineering issues. The results from the test and evaluation can be used in future research.

The process followed in the testing and evaluation of the artefact throughout this chapter is as follows:

1. Identify, and communicate with, participants who were involved in the prior participatory design workshops to obtain their participation in the artefact ***reaction*** evaluation;

2. Develop and distribute the ***reaction*** questionnaire feedback form that includes a link to play the final game-based artefact;

3. Identify, and request, new potential participants who fall within the target user group to take part in the ***learning*** evaluation of the artefact;

4. Develop and distribute the anonymous pre- and post-test online questionnaires (for the ***learning*** evaluation) to the identified participants (which can only be completed if consent is provided);

5. Present the analysed data results from the ***reaction*** and ***learning*** level evaluation; and

6. Complete the summative evaluation and testing of the game-based artefact

Section 7.2 provides an overview of the game-based artefact, which was iteratively developed in Chapter 6. Only the key design features of the game-based artefact are presented in this chapter.

Section 7.3 describes the *summative evaluation and testing* of the artefact using the four-level model for artefact evaluation by Petri and von Wangenheim (2016:995), which was described in Section 2.4.2. It is important to note that only two of the four levels (***reaction*** and ***learning***) from the model will be used to test the artefact. The ***reaction*** level evaluates how the participants feel about the design of the artefact, whereas the ***learning*** level evaluates whether a learning experience is prompted. These level results are discussed in Sections 7.3.1 and 7.3.2, respectively.

To review the ***reaction*** level of the artefact, the participants can interact with the artefact, and then provide their response regarding its design. The results are captured from the participants and are open-coded. The open-coded results are depicted in Section 7.3.1 as Table 7-4. The codes are grouped according to the identified themes used throughout the study (refer to Appendix J for an example of themes).

To review the ***learning*** level of that artefact, a pre-test questionnaire is provided to the participants regarding key social engineering concepts to determine their initial level of understanding. The participants are then required to play the game-based artefact, which is intended to teach them about the key social engineering concepts identified in this study. This is followed by a post-test questionnaire to determine their level of understanding after they have interacted with the artefact. The test of learning will then be to determine whether the participants' results have improved on the post-test after having interacted with the artefact. An improvement in the participants' post-test results would indicate that a learning experience has occurred after interacting with the artefact. Section 7.3.2 provides a summary of the learning evaluation results.

Section 7.3.3 discusses the *quality* evaluation criteria for the game-based artefact. The evaluation criteria are based on the criteria defined by Mckenney and van den Akker (2005:48). The evaluation criteria evaluate the **quality aspects for designing, developing, and evaluating** an artefact. Section 7.4 discusses whether any additions can be made to the research body of knowledge from the findings noted in this chapter. Section 7.5 concludes this chapter.

Figure 7-1 depicts the number of participants in the summative evaluation and testing of the artefact. This occurs in the last two loops, which are the *final evaluation* and *query* loops. Within

the context of this study, the ***summative evaluation & testing*** depicted in Figure 7-1 refers to the artefact testing and evaluation, where the *final evaluation* cycle in the figure refers to the ***reaction*** evaluation of the artefact and the *query* cycle in the figure refers to the ***learning*** test of the artefact.

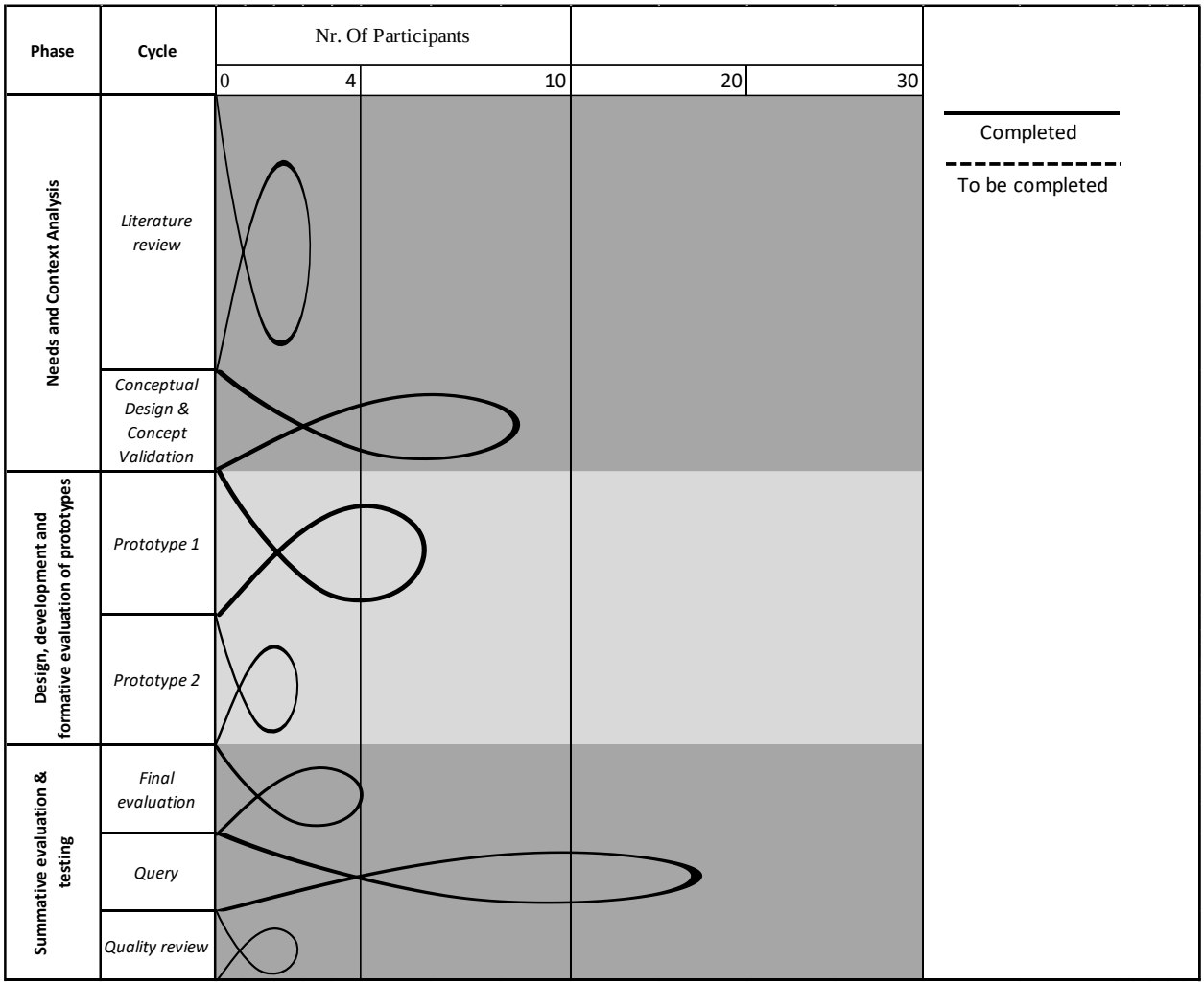


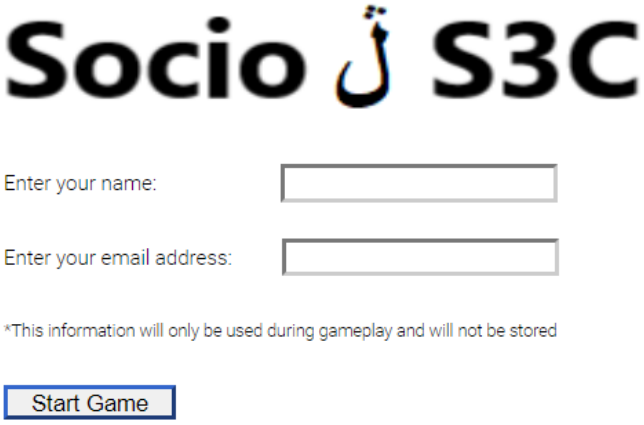
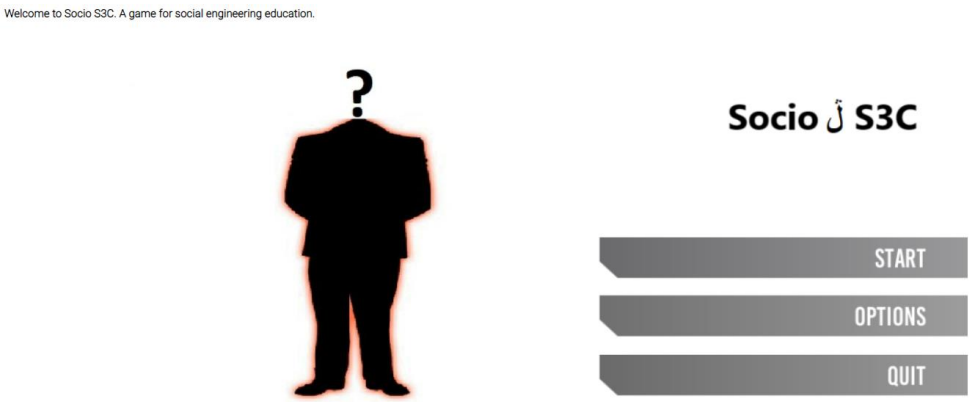
Figure 7-1: Research cycle for the final evaluation (reaction evaluation) and query (learning test) of the prototype artefact

7.2 Design overview of the game-based artefact

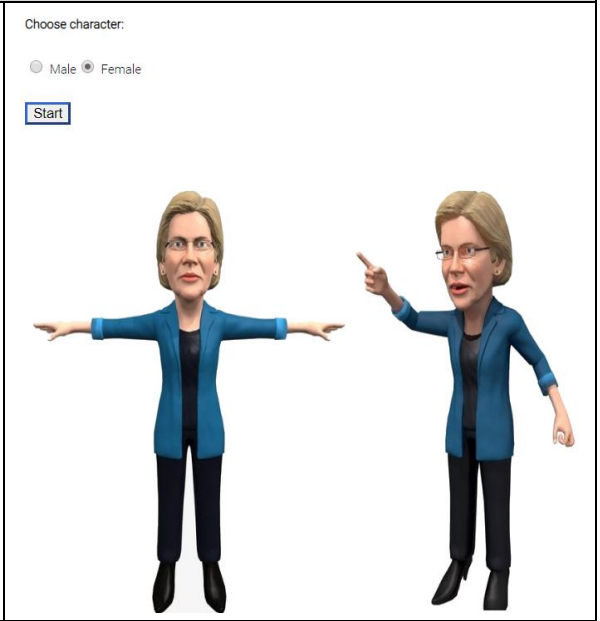
This chapter provides the results from the summative evaluation and testing of the game-based artefact. In order to provide context for the final artefact under evaluation, this section provides a non-exhaustive summary of the game-based artefact design outcomes. Table 7-1 provides an overview of the key design features of the game-based artefact. The game-based artefact was designed to depict six of the key social engineering concepts over five challenges. The six social engineering concepts are baiting, phishing, tailgating, shoulder surfing, watering hole, and

dumpster diving attacks. A description of each of the attacks was provided in Table 6-1. The final artefact can be accessed at the URL: https://socios3c.online/

Table 7-1: A summarised overview of the key design features of the game-based artefact

1. The screen displayed when you start the game at URL: https://socios3c.online/

2. The screen displayed after you start the game.


3. The screen that allows you to choose your character at the start of the game.



4. The screen that provides the player with a tutorial on what the game is about and how to play it.

5. The screen displayed when you complete the tutorial and spawn into the game world with the character you chose in exhibit 3.

Challenges visited: 0 of 5

Test, YOU HAVE JUST ARRIVED FOR YOUR FIRST DAY AT WORK

AS YOU CAN SEE, SECURITY IS TAKEN VERY SERIOUSLY!

Display game menu

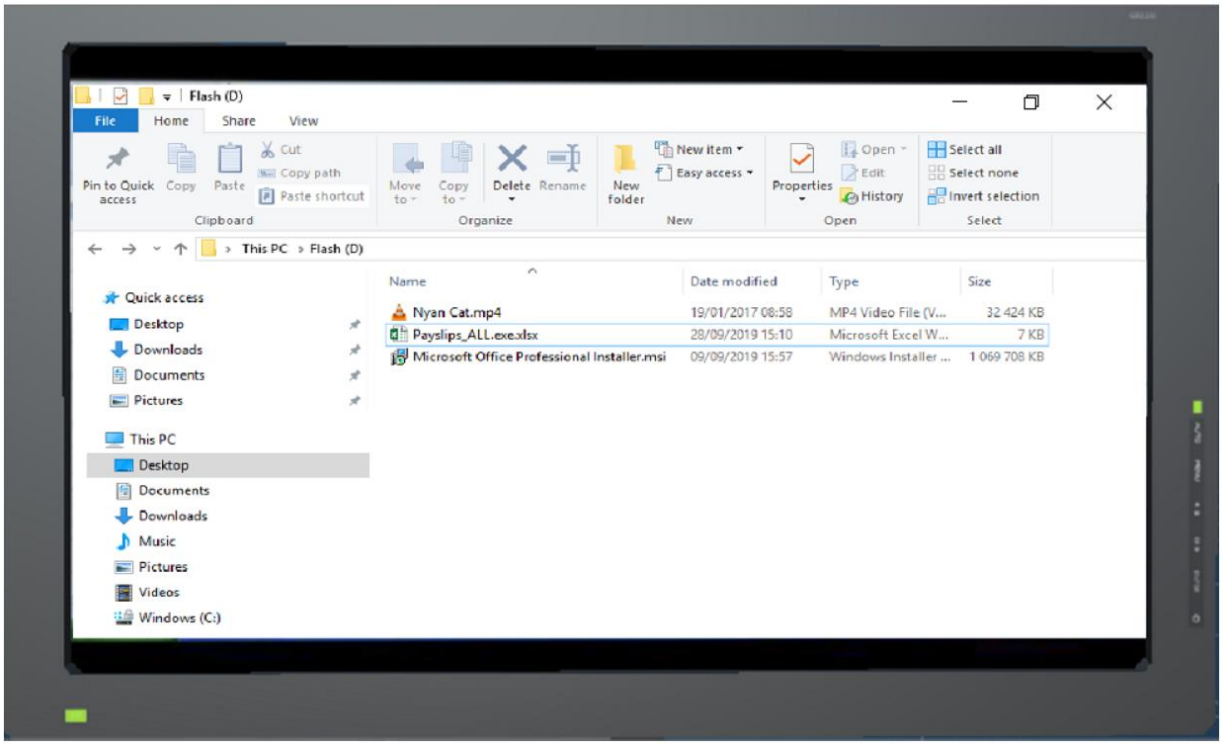
Hover your mouse over the image below to see what actions you can perform. You can click on the hovered area to perform the action.

6. The first challenge in the game, which represents the *baiting* social engineering concept.

Challenges visited: 1 of 5

YOU HAVE OPENED THE USB DRIVE ON THE COMPUTER

There seems to be some interesting files on this USB drive.



7. The second challenge in the game, which represents the *phishing* social engineering concept.

Challenges visited: 2 of 5

Continue

From: Facebook_Support <suppor@facebook.unlock.com>
Date: August 27, 2019 at 9:49 PM
To: test@test.com
Subject: !Security Alert!

facebook

Hi **test**,

We have noticed a security breach on your Facebook account, For your protection, your account has been locked out.

Please click on the link below to unlock the account:

Log-in to:
facebook.unlock.com

This matter needs your URGENT attention.

Sincerely,
The Facebook Team.

facebook

This email was sent to test@test.com. If you don't want to receive these emails from Facebook in the future or have your email address used for friend suggestions, you can unsubscribe. Facebook, Inc. P.O. Box 10005, Palo Alto, CA 94303.

8. The third challenge in the game, which represents the *tailgating* social engineering concept.

Challenges visited: 2 of 5

YOU ARE NOW ENTERING THE MEETING ROOM

Display game menu

9. The fourth challenge in the game, which represents the *shoulder surfing* social engineering concept.

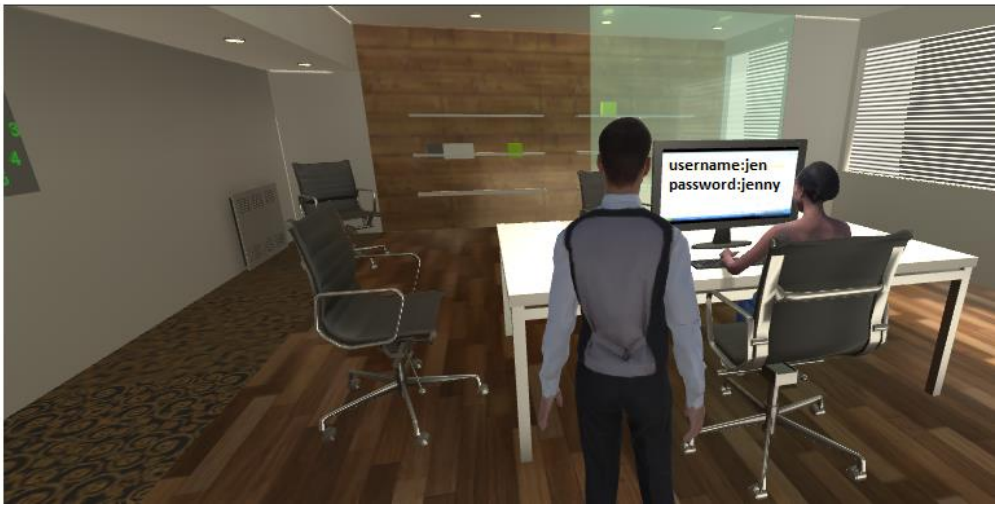
Challenges visited: 3 of 5

YOU ARE IN THE MEETING ROOM

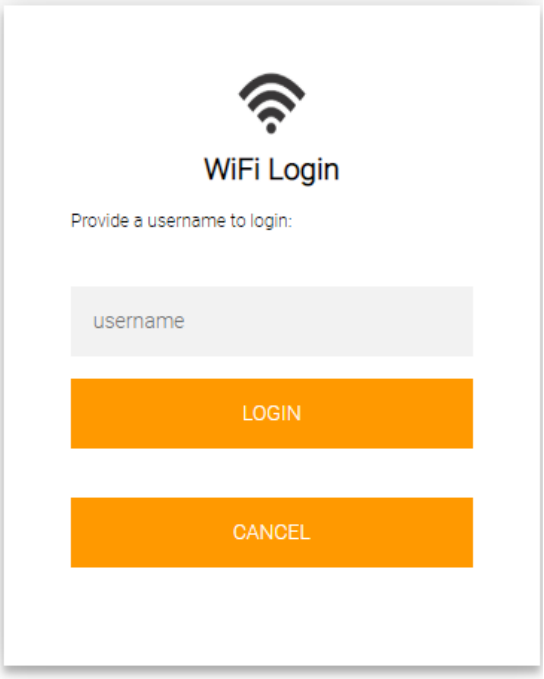
It appears Jen can't see you. Her username and password are on the screen.
This is known as SHOULDER SURFING.

Explore the other rooms for more challenges by going back.

Display game menu



10. The fifth challenge in the game, which represents the *watering hole* social engineering concept.



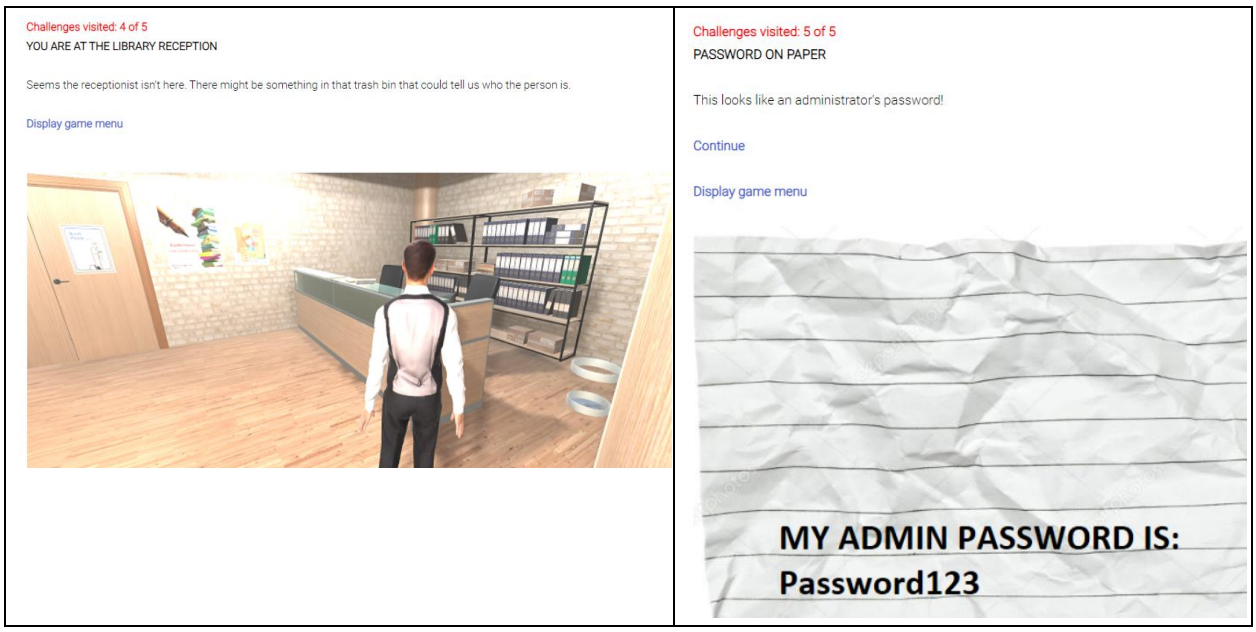
Challenges visited: 4 of 5

YOU HAVE FALLEN VICTIM TO A WIFI PHISHING ATTACK

Here's why

This is an example of a wifi phishing attack. This could also be seen as a watering hole attack as the website used to login to the wireless network has been compromised.

11. The sixth challenge in the game, which represents the *dumpster diving* social engineering concept.



7.3 Summative evaluation and testing

The summative evaluation and testing of the artefact is performed according to two levels of the four-level model for evaluating artefacts by Petri and von Wangenheim (2016:995). The summative evaluation and testing also evaluates the artefact *quality* according to the quality aspects for designing, developing, and evaluating an artefact by Mckenney and van den Akker (2005:48).

The two evaluation levels used are the ***reaction*** and ***learning*** levels, which are depicted in Table 7-2. The reason for only using the two levels from the four is due to the process followed in the development of the artefact, which allows the artefact to only be evaluated as a once-off assessment at the end of its development and not over an extended period. The *behaviour* and *results* evaluation levels require that the artefact be implemented and assessed over an extended period. This is not possible within the scope and limitations of this study. Section 7.3.1 and Section 7.3.2 will discuss the ***reaction*** and ***learning*** levels in greater detail.

Table 7-2: The four-level model for evaluating educational artefacts (Petri & von Wangenheim, 2016:995)

Evaluation	Evaluation description and characteristics	Examples of evaluation methods and instruments
Reaction	Evaluating how participates feel about the learning experience brought about by the artefact	Questionnaires, verbal responses, as well as feedback forms

Learning	Evaluates whether the participant's knowledge or skills have improved	Pre- and post-test reviews before and after the training, observations, as well as interviews
Behaviour	Evaluates the extent of change in actions (behaviour) brought about by the learning experience over a long term	Interviews as well as observations which are conducted over a long term
Results	Evaluates how the participants impact the business environment after being introduced to the artefact	Interviews as well as observations on participants, managers, etc. and are conducted and measured over a long term

7.3.1 Reaction evaluation

This section evaluates how the participants felt about the game-based artefact. The participants interacted with the artefact and provided feedback regarding its design. The responses are open-coded according to the themes defined in prior chapters of this study. The approach to open coding follows a similar approach as used by Romand Jr *et al.* (2003:222) in their research article titled '*A methodology for analyzing web-based qualitative data*'. The open-coded results are depicted in Table 7-4.

7.3.1.1 Overview of process

In order to obtain the ***reaction*** evaluation of the participants, the game-based prototype had to be completed. The initial plan was to obtain the results from the participants in a participatory design workshop where the participants would be allowed to interact with the artefact and then provide feedback through a participatory design workshop, similar to the process used in prior workshops. The questions would be based on questions generally asked during playtest feedback sessions. Examples of these questions are accessible at resources by Patton (2017) and Anonymous (2020). However, due to the COVID-19 pandemic, it was not possible to conduct the participatory design workshop and an alternative approach was used. The alternative approach was to supply the participants with a link to the game and an online form containing a set of open-ended questions that could be used to obtain the rich feedback.

In order to obtain the participant responses, the participants are contacted via email to play the game-based artefact and to complete the feedback form. The feedback form contains the same questions that would have been posed to participants during a participatory workshop. The participants invited to take part in the ***reaction*** evaluation feedback had participated in a prior workshop in this study, where their role was to inform the design and development of the artefact. The reason for using the same participants for the ***reaction*** evaluation is that the participants were intimately involved in the development of the artefact and had a clear understanding of the

purpose of the study and why the artefact was developed. The participants could also provide richer feedback on whether the artefact adequately addressed the requirements that were defined by them during the design and development of the artefact. It is important to note that during participatory workshops, different types of participants are included as rich feedback on the design elements and design experience is required. Table 7-3 provides an overview of the participants who formed part of the ***reaction*** level evaluation. Further detail on the breakdown of all the participants involved in this study is summarised in Appendix D.

Table 7-3: Participants involved in the reaction level evaluation of the game-based artefact

Reaction participant #	Feedback role	Field	Years of experience in role
RP1	Administrative/support role	Academic sector	6 years
RP2	Design expert	Academic sector	9 years
RP3	Design expert	Academic sector	4 years
RP4	Cyber-security professional	Industry sector	4 years

The evaluation form containing the open-ended questions indicated that participant detail would be kept anonymous and therefore did not capture any identifying information. The questions are grouped according to the themes identified in the initial workshops, which included detail such as the platform design, character design, user interface design, and mechanics of the artefact. These themes were used in building the conceptual prototype and the functional prototype (Chapters 5 and 6). An example of the open-ended feedback form used in this ***reaction*** evaluation is depicted in Appendix O. The section that follows provides further detail on the results from the analysis of the open-ended questions.

7.3.1.2 Feedback

The feedback from the responses is reviewed, and open coding is used to sort the data according to themes. No new themes were identified during this process as all data could be grouped under the existing themes identified in this study. The results of the open coding are depicted in Table 7-4.

Table 7-4: Reaction evaluation of the themes identified in the coded participant responses during the final game-play

Code	Description within context of workshop feedback
Theme 1: Platform	
The game provides a good learning experience (3 occurrences)	The game provides the learning experience that was intended.
The game is easy to play on the given platform (1 occurrence)	It is easy to play the game on the given platform.
The game addresses the platform requirements (2 occurrences)	The artefact was designed in a way that was suitable for the platform it was deployed on.
The game is unresponsive on the given platform (3 occurrences)	The game content took long to load in some instances, which made it unresponsive and sometimes required the player to restart the game.
Theme 2: Character	
The character designs do not represent real-world people appearances (2 occurrences)	The character selected does not closely represent a real-world person, i.e. the character in the game does not represent the features of a real person.
There should be more character selection options (2 occurrences)	The game should allow the player to choose a greater variety of characters or have the ability to create their own.
The character designs are acceptable (2 occurrences)	The character design is suitable for the given platform and the intended purpose.
The character designs do not offer enough culture variations (2 occurrences)	The characters of the game do not adequately represent the variety of cultures, which include colour, age, ethnicity, etc.
Theme 3: Mechanics	
The challenges are not obvious enough (6 occurrences)	The challenges are not obvious and distinct enough for a non-technical person to identify. A player needs to randomly click and guess until they reach the challenge.
The timed text is not aligned to the voice-over audio (1 occurrence)	The timed text during the gameplay does not align to the voice audio. The text should be displayed completely or allow the user to skip through all of it promptly.
The initial instructions are not clear (4 occurrences)	The instructions at the start of the gameplay lack clarity and do not provide the player with sufficient detail.

Code	Description within context of workshop feedback
There are no clear instructions on how to continue during the game-play (13 occurrences)	There is no clear direction on when and how to continue with the game-play, i.e. the game should offer continuous instruction and visual cues to the player on how to proceed with the game-play.
There is no game over indication (2 occurrences)	The game does not indicate when it is over after all the challenges are complete.
The character should be visible even during the play of the challenge (1 occurrence)	The game should allow the character to be visible even during interaction with the different challenge components, e.g. the character should be displayed when working on the keyboard during the phishing challenge.
The character movement is restricted and therefore linear (3 occurrences)	The game movement is restricted to only two buildings, which makes the game progression linear.
The storyline seems random (3 occurrences)	The game scenarios are disjoint and random. There are no markers or other visual cues that pertain to the overall objectives of the game. This makes the mechanics of the game almost redundant.
The scoring system does not add any value to the game-play (2 occurrences)	The scoring system is lacklustre and does not add value to the learning experience.
The game lacks supplemental resources (1 occurrence)	The game does not include supplemental resources during the gameplay. The inclusion of additional supplemental resources (links, tools, documents, external portals, etc.) will allow for more interaction for a curious player.
The Facebook challenge is clear and interactive (5 occurrences)	The interaction with the Facebook email challenge is clear, as instructions to play the challenge are provided, options are presented to the player to decide the correct answer from the available options, and a clear answer is provided as feedback.
The start game menu should have more options (1 occurrences)	The start game menu should have additional elements in order to change the appearance and behaviour of the game.
The game should allow the player to play in full-screen mode (1 occurrence)	The game should allow a player to select a full screen mode setting.
The game should have background music (1 occurrences)	Adding background music may make the game more appealing to the player.
The mechanics on the user interface (UI) are simple to interact with (1 occurrence)	The UI mechanics are easy to interact with, but could be improved.
Theme 4: UI design	

Code	Description within context of workshop feedback
There are inconsistencies in the resolution, aspect ratio and fonts of the artefact (3 occurrences)	The aspect ratio and resolution of the images are not consistent between scenes. The font is also not consistent between scenes.
The game information can be realigned for better reading (1 occurrence)	The in-game information should be moved around so that it can be read better, e.g. moving the text from the left of the screen to the centre as it will be easier to identify by the player.
A two-dimensional (2D) game design is preferred (4 occurrences)	The use of the 3D game design makes it difficult to identify the available interaction points on the user interface.
There is not enough detail available on the interaction points (5 occurrences)	The game does not clearly indicate the interaction points available on the user interface.
The elements of the game are not always aligned with the theme (1 occurrence)	Elements in the game do not align with the theme, e.g. the characters look cartoonish while the game setting represents a real-world environment.
The UI design is adequate (2 occurrences)	The UI design adequately addresses the design requirements.
The UI can be improved (3 occurrences)	The user interface should be made more user friendly.

From the open-coded results listed in Table 7-4, there are definitive areas of improvement for the artefact. From a *platform* theme perspective, it is clear that the platform is appropriate for the type of artefact presented. However, there are various issues regarding the responsiveness of the application at certain scenes during the gameplay, where the artefact becomes slow or unresponsive. This performance issue could be improved by resizing the quality of the images used in the game-based artefact to a lower quality or by redeploying the virtual machine hosting the game-based artefact to a region closer to the target audience location (which is South Africa) – this could reduce network latency. Additional improvements could be to use a content delivery network (CDN) such as Cloudflare to host the video content, which would improve video throughput when video content is delivered to more than one user simultaneously requesting the video content. Alternative to the above improvements is to use the Microsoft Azure blob storage to host all the image and video content. The Azure blob storage offers high performance for delivering throughput demanding content, but comes at a cost.

From a *character* theme perspective, the participants indicated that there is not a sufficient variety of characters to choose from. The character designs did not adequately represent the varying

cultures that players would be able to relate to. Additionally, the character designs did not represent real-world people, but looked more cartoonish. A design improvement would be to allow a player to custom create their character by allowing the player to customise character features such as the skin, hair, gender, physical size, etc. that would make the character more appealing to the player.

The *mechanics* theme of the artefact indicated that much future work could be done to improve the artefact. A topic that came across was that the game-play instructions were not presented strongly enough. The tutorial at the start of the game did not sufficiently emphasise the objective of the game as well as how the character should manoeuver around the world. The in-game instructions did not provide the player with enough cues to proceed through the game, which made players end up getting stuck in different stages of the game and consequently restarting to get out of the blocked stage. It is also clear that the challenges were not represented clearly enough, which meant users needed to guess whether the interaction would lead to a challenge or not. This resulted in challenges being missed. Other aspects that also came across were that the game did not adequately indicate when it was over, and the storyline was random and had no clear path as to what the final objective is. The character movement was also limited in terms of where the character can go and what it can interact with. Some suggestions for improving the mechanics were to improve on the representation of the instructions pre-gameplay and during gameplay. Adding music would enhance the gameplay, and allowing the player to switch the game to full screen would help immerse the player in the game. An additional suggestion was that supplemental resources should be included throughout the game. The supplemental information could be in the form of unified resource links (URLs), PowerPoint presentations, documents, etc. embedded in the game, which can allow the player to access more information relevant to the social engineering topics depicted in the artefact.

The last theme, which relates to the *user interface* (UI) design, indicates that some participants preferred the game to be two-dimensional (2D). The participants also point out a very important aspect of the game design, which is that the game did not clearly indicate the interaction points for the heat maps on the images, i.e. the heat maps were not clearly identifiable on the images they were embedded on. This requirement could not be implemented due to a design limitation of the image-map function in the hyper-text mark-up language (HTML). Image-map does not allow the highlighting of mapped areas on the image, which, if possible, could have been used to provide the player with an indication of the interaction points on the images. An additional issue identified was that there were some inconsistencies in the font design and image sizes when moving between scenes in the game.

In summary of the above, it is clear that the biggest concerns on the game design are that:

1. there are limited instructions available to guide the user on what to do or where to go during the gameplay;

2. the objective of the game is not clearly defined, which made the player struggle to navigate through the different challenges of the game;

3. the character manoeuvrability is limited and needs to be improved to allow the character to interact freely with more objects in the game world;

4. the challenges should be made more obvious to the player; and

5. the interaction points on the image heat maps need to be improved in such a way that the player can easily distinguish the available clickable (interactive) areas.

It is also worth summarising the positive feedback received from the participants. This was mainly regarding the platform being fit for purpose, the game being easy to play, and the game bringing about a learning experience. The participatory design workshops performed in Chapters 5 and 6 indicated that the suitable platform to present the game-based artefact was for a computer-based platform delivered over a web browser. The reason for allowing the game-based artefact to be accessible over a web browser is to allow the game to be accessed from any location using the Internet. The game-based artefact was presented in the form of a storyboard style using Twine 1.4.2. This is a requirement gathered during the participatory design workshops. The reason for presenting it in a storyboard style made it easier to interact with the artefact as this style was more preferred by the target user group, which are people working in administrative roles. The section that follows seeks to determine whether a ***learning*** experience occurred for the participants.

7.3.2 Learning evaluation

This section evaluates the ***learning*** experience of the participants after playing the game-based artefact. The participants are presented with a pre-test questionnaire to complete, then play the game-based artefact, and finally complete an identical post-test questionnaire. The results from the pre-test and post-test are compared, the comparison of which will determine the ***learning*** experience achieved by the participants. Typically pre- and post- test questionnaires follow a more quantitative approach. Participants who are involved in such questionnaires are commonly referred to as respondents, however, because all the participants which were involved in this study formed part of a participatory design strategy, they are therefore referred to as participants.

7.3.2.1 Overview of process

In order to determine the ***learning*** that took place after interaction with the artefact, a pre- and post-test questionnaire is presented to the participants to complete. The pre- and post-test questionnaires are made up of a series of questions that relate to social engineering issues. The questionnaires are structured according to the approach followed by Jerry Chih-Yuan *et al.* (2017:48), where a pre-test was performed on participants, an artefact was presented to them, then a post-test was performed to determine whether a learning experience had taken place. Similar to the ***reaction*** evaluation, the intention was also to present the ***learning*** evaluation as a participatory design workshop (as workshop 4). However, due to the COVID-19 pandemic, it was not possible to conduct the participatory design workshop and an alternative approach was used. The alternative approach was to supply the participants with a link to the game-based artefact and a link to the pre- and post-test questionnaires that could be used to obtain the ***learning*** evaluation feedback.

The social engineering concepts that are presented in the questionnaires are an excerpt from the social engineering concepts identified in the literature in Section 3.2.4 of Chapter 3. The questionnaires are designed in such a way that it can present the key social engineering concepts that are illustrated in the game-based artefact. Both questionnaires are identical for the purpose of accurately measuring whether the artefact improves the participants' understanding of the social engineering issues presented. The questionnaires are listed in Appendix M (pre-test) and Appendix N (post-test). The structure of the questionnaires used in this study is based on the structure used in the pre- and post-test questionnaires in the study by Jerry Chih-Yuan *et al.* (2017:58). The pre-test assesses the level of social engineering awareness of the participants before they interact with the artefact.

The participants used in the ***learning*** evaluation are participants who have not formed part of any prior participatory workshops. The reason for this is that using participants who were involved in prior workshops would not provide an accurate measure of the learning experience that may take place when the participants interact with the artefact and complete the questionnaires. This inaccuracy would primarily be because the participants would already be aware of the social engineering concepts that would have been presented in the prior workshops and it is assumed that they would score better results in both tests.

Once the participants have completed the pre-test questionnaire, they are prompted to play the game-based artefact, which is expected to bring about a learning experience in the participants. The post-test questionnaire assesses whether a ***learning*** experience has taken place after having played the game-based artefact. This is achieved by performing a comparison of the pre-

test and post-test results. The participants identified are those who fell within the administrative role from a medium to large organisation. The participants are mainly secretaries, general business administrators, finance and accounts administrators, as well as internal business reputational risk administrators. The questionnaires and artefact are communicated with the potential participants through email for them to complete. Seventeen participants are identified and contacted, of which 15 are able to complete the questionnaires. The results from the questionnaires are compared in the section that follows.

7.3.2.2 Results

The participant results from the pre- and post-test questionnaires are summarised in Table 7-5. The table depicts the pre-test scores and the post-test scores for each participant with an indication of whether a learning experience took place.

Table 7-5: Comparison of the pre-test and post-test results

Learning participant # (LP)	Pre-test score	Post-test score	Result (increase/ decrease/no change)
LP1	18 / 25	24 / 25	↑
LP2	20 / 25	22 / 25	↑
LP3	21 / 25	21 / 25	↔
LP4	16 / 25	19 / 25	↑
LP5	21 / 25	22 / 25	↑
LP6	15 / 25	18 / 25	↑
LP7	20 / 25	22 / 25	↑
LP8	16 / 25	17 / 25	↑
LP9	17 / 25	13 / 25	↓
LP10	17 / 25	17 / 25	↔
LP11	18 / 25	17 / 25	↓
LP12	21 / 25	22 / 25	↑
LP13	21 / 25	21 / 25	↔
LP14	20 / 25	18 / 25	↓
LP15	12/25	20 / 25	↑

A summary of the results depicted in Table 7-5 indicates that, out of the 15 participants, nine (60%) achieved a learning experience from the game play, three (20%) experienced no increased learning, and another three (20%) had a decline in their scores. These results are summarised

as Figure 7-2, which provides a summary of the results for the change in awareness of the participants.

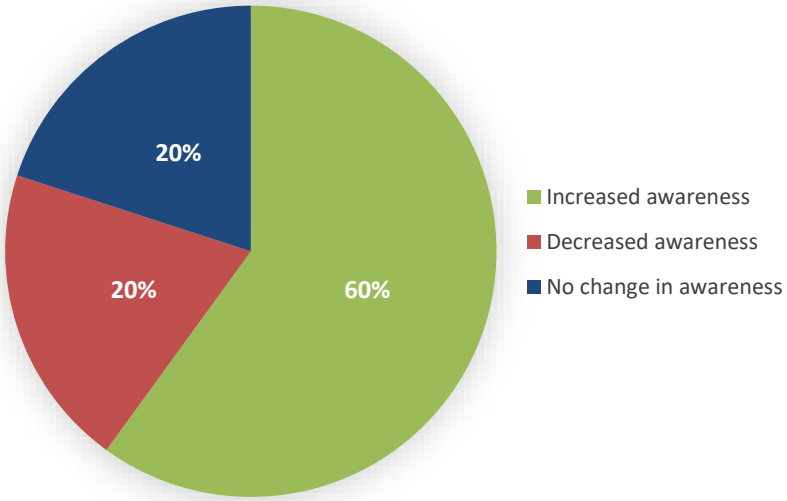


Figure 7-2: Summary of the social engineering awareness changes in the participants

It is not clear why the decline occurred for the three participants, but it could be due to distractions as it was observed in the feedback timeline that the participants had completed the questionnaire over several days. In the post-test, a single open-ended question was presented at the end of the questionnaire so that the participant could share any comments or feedback after having interacted with the game-based artefact. Of the 15 participants, four responded to the open-ended question. One of the four participant responses indicated that the game was useful, whereas one other indicated that it was not possible to complete all five of the challenges due to one of the challenges being difficult to find. The remaining two participants (of the 17 that were contacted) had started the pre-test questionnaire and game-play, but had not completed the post-test questionnaire. The participants who had not completed the post-test questionnaire were contacted to understand the particular reason for not being able to complete it. The reason provided by one of the participants was that there was a technical problem on their device and he could therefore not complete the post-questionnaire. The other participant could not be reached for feedback on the non-completion.

Table 7-5 provided a comparison of the results of the pre- and post-test that was performed with the participants. The test aimed to determine whether a better understanding of the social engineering attack types had occurred after participants interacted with the artefact. The results indicate an increase in the participants' understanding of the social engineering concepts post the

gameplay. It is clear that the game-based artefact has brought about a learning experience in the participants. The section that follows aims to evaluate the *quality* aspects of the artefact and is based on the quality criteria defined by Mckenney and van den Akker (2005:48).

7.3.3 Artefact quality evaluation criteria

As described in Section 4.4.2.3 of Chapter 4, the artefact evaluation occurs in the form of a field trial where it is evaluated to determine whether it meets the objectives for which it was developed.

Table 7-6 is a representation of the table used in the study by Mckenney and van den Akker (2005:48) to evaluate the *quality* aspects of an artefact (which was referred to as the CASCADE-SEA program). Table 7-7 maps the quality aspects depicted in Table 7-6 to the game-based artefact developed in this study (referred to by its name, SOCIOS3C).

Table 7-6 depicts the *traits* and *quality* aspects of an artefact. The traits for evaluating the game-based artefact are the *content*, the *support* offered to the player, and the technical *interface* of the artefact. These criteria provide the traits for evaluating the game-based artefact.

The *quality* of the artefact is evaluated according to three criteria, which are the validity, practicality, and impact potential. ***Validity*** refers to state-of-the-art knowledge offered in an internally consistent fashion. For SOCIOS3C, the *state-of-the-art knowledge* relates to the development of unique qualities in the game-based artefact. *Internal consistency* refers to how the content, support, and technical interface remain aligned throughout the design of the artefact. ***Practicality*** refers to the way the tool fits and contributes to the target setting. The *instrumentality* quality refers to providing procedural specifications for implementing exemplary design material in the artefact. The *congruence* quality refers to the fit between the proposed and prevailing conditions in the design. The cost quality refers to the cost benefit obtained in the development of the artefact. ***Impact potential*** refers to the potential change the game-based artefact can bring about to the player. This is divided into the observation of whether the game-based artefact *yields better quality material*, which translates to whether quality of the materials used in the artefact can be impactful to the player. It is also used to assess whether the game-based artefact *enhances the professional development* of the player, which translates to whether a learning experience can be achieved based on the traits of the artefact.

Table 7-7 is an adaptation of Table 7-6 and maps the quality and traits to the context of evaluating the design and development of the SOCIOS3C game-based artefact. Table 7-7 therefore summarises the quality aspects of the game-based artefact developed throughout this study.

Table 7-6: Quality aspects for designing, developing and evaluating the CASCADE-SEA program by Mckenney and van den Akker (2005:48)

	Traits / Quality	Content	Support	Interface
Validity	State-of-the-art knowledge	Curriculum design and development knowledge; Related professional development knowledge	Advice on materials design; Guidance on embedding materials in professional development	Maximise the potential of modern ICT facilities
	Internally consistent	Ideas in various components are in line with those in other areas	Tips guidelines, templates, advice, and help functions are perpetually offered in a consistent fashion	Functions as intended, regularly
Practicality	Instrumentality	Guides the user step-by-step in making materials; offers freedom to work at own pace and in own style	Explains how to use program clearly and concisely	Buttons, navigation, and functions are clear
	Congruence	Links up with the needs, wishes, and context of the users	Support is relevant and usable	Interface 'feels' nice and safe, users are not alienated, but motivated to use the program; Operates on technology that is available in the target setting
	Cost	Content should include enough of what users need, and not bog them down with unnecessary steps	Support should be extensive, lowering the threshold of investment cost of the user	Interface should reflect the flexibility of the system, in which users determine how they would like to go through the program (maximum degree of freedom, minimum allowance for error)
Impact potential	Yields better quality materials	The materials that are developed through the use of the CASCADE-SEA should be valid, practical, and effective	The materials that are created with the CASCADE-SEA should contain clear, useful procedural specifications	The materials that are generated with the CASCADE-SEA should evidence attention given to form and style
	Enhances the professional development of users	CASCADE-SEA should help users to think about the materials development in a (more) systematic and thorough fashion	Teaches users where resources can be found (inside the program), and how they may be used and/or adapt for own setting	Interface helps (teams of) users to visualise the process of materials development and make their work more transparent

Table 7-7: An adaptation of the evaluation of the quality aspects for designing, developing, and evaluating SOCIOS3C

	Traits / Quality	Content	Support	Interface
Validity	Professional knowledge	The content used in SOCIOS3C is developed using professional materials obtained from the Unity asset store and modified or developed using Blender as a modelling tool	The support received in developing SOCIOS3C was guided by research experts who advised on using professional game design platforms such as Twine and Unity	The hosting of SOCIOS3C uses professional online platforms such as the cloud and uses professional delivery and protection mechanisms such as Cloudflare routing and DDoS protection
	Internally consistent	It was indicated in the feedback received in Section 7.3.1.2 that the design of SOCIOS3C had room for improvement in that the aspect ratio, resolution, and font were not consistent in the interface design	Help functions are not consistently provided and there is room for improvement, this is depicted in the feedback received in Section 7.3.1.2	SOCIOS3C functions as intended, regularly with minor lags in content delivery to some users
Practicality	Instrumentality	The game is playable, but lacks clarity in the gameplay instructions. The player is not rushed and can play at his own pace. The player is also able to save the game and resume it later	As indicated in the feedback received in Section 7.3.1.2, the initial instructions on how to play the game are not clear, and need to be improved for clarity	As indicated in the feedback received in Section 7.3.1.2, the artefact needed improvement on the heat map interaction points on the user interface
	Congruence	SOCIOS3C provides the minimum needs, wishes, and context of the users, but could be improved from a mechanical and user interface perspective	The game support is relevant and usable, but could be improved by adding cues at specific scenes	The interface is simple enough for the users to interact with, but lacks clarity on the areas they are able to interact with during certain scenes. This issue creates frustration for players
	Cost	The content was sufficient and presented the material adequately	As indicated in Section 7.3.1.2, the support should be improved. This will be at a cost of additional development time	As indicated in the feedback received in Section 7.3.1.2, SOCIOS3C lacks the ability to allow the character to freely move and interact with different objects in the game. There is room for improvement
Impact potentia	Yields better quality materials	The quality of the materials was iteratively improved	The materials used in the design of SOCIOS3C can be	The materials used in the design of SOCIOS3C could be

	Traits / Quality	Content	Support	Interface
		with the design experts and design artist. This is discussed in Chapter 6 throughout the development cycles of the prototype	improved based on the feedback received from the participants in the reaction evaluation	improved to better interface with the platform, such as keeping design consistency and allowing it to be used in a full screen mode
	Enhances the professional development of users	SOCIOS3C allowed the users to achieve a learning experience as was depicted in the results of Section 7.3.2.2	As per the open-coded results in Section 7.3.1.2, SOCIOS3C lacked the ability to adequately support the development of the player in that sometimes players got stuck during the gameplay	The interface of SOCIOS3C needs improvement; however, from the results in Section 7.3.2.2, it does enhance the development of the player's understanding of social engineering concepts

7.4 Additions to the knowledgebase

At this stage of the study, additions to the knowledge base were a conference paper titled '*Raising social engineering awareness through gameplay'* which was submitted to the 19th World Conference on Mobile and Contextual Learning (mLearn) on August 1st, 2020 and was presented with the proceedings forthcoming. Proof of submission for the conference paper can be found in Appendix P. This addition brings the total conference papers submitted to two, with the first paper submitted in Chapter 5 (Section 5.4.2). Other additions are that Google Forms was used as a platform to administer the pre- and post-test questionnaires and it worked well. The approach used to test and evaluate the artefact as described in Section 7.3 also worked well.

Table 7-8 provides a description of the legend presented in Table 7-9. Table 7-9 follows from Chapter 2 of this study (the literature review) up until this chapter, which is the summative evaluation and testing of the artefact. The table depicts the circuits (iterations) that have been followed until this point, with all of the participants involved in each of the circuits. Table 7-9 should be read in conjunction with Figure 7-1, as Figure 7-1 is a summary of the process followed and the cycles.

Table 7-8: Description of the legend depicted in Table 7-8

Legend item	Description
Strategies (strategies used in the cycle)	
RE=Reaction evaluation	An evaluation that aims to determine how a participant feels about the artefact.

Legend item	Description
LE=Learning evaluation	An evaluation that aims to determine whether there is a learning experience in the participant using the artefact.
AD=Artefact development	Time spent developing the artefact by the developer.
EA=Expert appraisal	Time spent by an expert performing as assessment of a circuit component.
ME= Micro evaluation	An evaluation case at a particular circuit.
TO= Tryout	Testing of the artefact by a user.
Users (users involved in the circuit)	
AIP=Academic institution participants	Participants from an academic institution who provide design inputs.
CIP=Corporate institution participants	Participants from a corporate institution who provide design inputs.
Experts (experts involved in the circuit)	
DSRE=Design science research experts	Design science research experts (from academia) who provide expert feedback at a particular circuit.
DA=Design artist	A design artist who provides expert feedback on the design elements at a particular circuit.
CSE=Cyber security expert	A cyber security expert who provides expert feedback on cyber security issues at a particular circuit.

Table 7-9: Overview of the strategies used over seven cycles consisting of 22 circuits until the completion of the artefact summative evaluation and testing

Phase	Cycle	Circuit	Strategy						Participants					#
									Users		Experts			
			AD	*EA*	*ME*	*TO*	*RE*	*LE*	*AIP*	*CIP*	*DSRE*	*DA*	*CSE*	
Needs and context analysis	*Literature review*	1												1
		2												2
		3												2
		4												2
		5												2
		6												2
		7												2
		8												1
		9												2
	Conceptual design & concept validation	10												2
		11												6
		12												3
		13												3
		14												6
Design, development and formative evaluation of prototypes	*Prototype 1*	15												2
		16												2
		17												4
	Prototype 2	18												2
		19												2

summative evaluation and testing	*Final evaluation*	20												4
	Query	21												15
	Quality review	22												2
Totals:			**9**	**12**	**6**	**4**	**1**	**1**	**3**	**3**	**18**	**3**	**1**	**61**
Estimated total participants when corrected for those who participated more than once:														**27**

Legend: =Strategies used = Types of participants

Strategies: RE=Reaction Evaluation; LE=Learning Evaluation; AD=Artefact Development; EA=Expert Appraisal; ME=Micro Evaluation; TO=Tryout
Users: AIP=Academic Institution Participants; CIP=Corporate Institution Participants
Experts: DSRE=Design Science Research Experts; DA=Design Artist; CSE=Cyber Security Expert

7.5 Conclusion

Table 7-10 outlines the process followed for the summative evaluation and testing of the artefact. It depicts the process for performing the ***reaction*** evaluation, the ***learning*** test on the participants, and the artefact *quality* evaluation criteria.

Table 7-10: An outline of the summative evaluation and testing of the game-based artefact

Step	Step description	Approach followed in the step
1	Identify, and communicate with participants who were involved in the prior participatory design workshops to obtain their participation in the artefact *reaction* evaluation	The participants who were involved in the prior participatory design workshops were identified, contacted via email, and asked to participate in the ***reaction*** evaluation of the final prototype. It is important to use the participants involved in the prior workshops, as they would be most suitable to provide feedback on the artefact design. The participants were suitable because they were intimately involved in its development and clearly understood the purpose of the study.
2	Develop and distribute the ***reaction*** questionnaire feedback form that includes a link to play the final game-based artefact	The ***reaction*** questionnaire was developed. The resources used to guide the design of the questionnaires were from Patton (2017) and Anonymous (2020). The questionnaire aligned to the themes used in the open coding throughout the development of the artefact in this study (see Appendix J for an example open-coded results table or Section 7.3.1.2 of this chapter for the open-coded results). The participants were provided with the URLs to the reaction questionnaire as well as the game-based artefact. The participants were required to first play the game located at URL: https://socios3c.online/ before completing the reaction questionnaire.
3	Identify, and request, new potential participants who fall within the target user	Participants who were not part of the prior participatory design workshops were identified and asked to participate in the ***learning*** evaluation of the game-based artefact. The reason for using a different set of participants who were not involved in the artefact design and

Step	Step description	Approach followed in the step
	group to take part in the ***learning*** evaluation of the artefact	development workshops is that performing the pre- and post-test would provide more accurate results. The participants would not have any context as to what the study is about and would most likely not be familiar with most of the social engineering concepts depicted in the artefact. The interaction with the artefact was expected to bring about the learning experience.
4	Develop and distribute the anonymous pre- and post-test online questionnaires to the identified participants (which can only be completed if consent is provided)	The pre- and post-test questionnaire was derived from the social engineering concepts that were illustrated in the gameplay. The questions are an excerpt from the social engineering attack types depicted in Table 3-6 of Section 3.2.4. The participants are presented with a link to the pre-test questionnaire, the game-based artefact, and the post-test questionnaire. The pre-test and post-test questionnaires are identical. Making the two tests identical is important to allow a higher accuracy in the results when comparing the knowledge of the participants before they interact with the artefact, and after. All the answers to the questions in the questionnaire are explained in game-based artefact. Consent was obtained from the participants at the start of the questionnaire. No paper-based forms were completed by these participants as a workshop could not be held with them due to the COVID-19 outbreak; therefore, all communication needed to be performed electronically.
5	Present the analysed data results from the ***reaction*** and ***learning*** level evaluation	The quality of the artefact was evaluated against the artefact quality testing aspects for designing, developing and evaluating the CASCADE-SEA program by Mckenney and van den Akker (2005:48). These artefact quality evaluation aspects are discussed in Section 7.3.3 and summarised as Table 7-7.
6	Complete the summative evaluation and testing of the game-based artefact	A summative evaluation and test was performed on the artefact in Section 7.3 where it was evaluated for *quality* against the artefact evaluation criteria defined by Mckenney and van den Akker (2005:48). The results from the questionnaire for the ***reaction*** evaluation of the artefact were analysed using open coding and are presented as Table 7-4 in Section 7.3.1.2. The results from the questionnaire for the ***learning*** evaluation of the artefact are presented as Table 7-5 in Section 7.3.2.2.

This chapter has provided an overview of the final game-based artefact, which was iteratively developed in Chapter 6. The artefact was evaluated and tested using two of the levels of the four-level model for evaluating artefacts by Petri and von Wangenheim (2016:995). The two levels evaluated and tested the ***reaction*** and ***learning*** aspects of the artefact, where the ***reaction*** level assessed the way the participants felt about the artefact, and the ***learning*** assessed the understanding that was brought about by the artefact.

From the ***reaction*** results in Section 7.3.1.2, it was clear that the artefact had room for improvement in terms of the user interface design, but more specifically on the mechanics. The mechanical requirements indicated that the artefact was not easy to interact with, lacked cues in the game, and often left players disoriented on what actions to perform to get into or past a challenge. The storyline of the artefact was also somewhat linear, and did not provide adequate

randomisation in the playability such as interacting with random objects or finding challenges in randomised locations.

From the ***learning*** evaluation results in Section 7.3.2.2, it was clear that there was room for improvement for the design of the artefact. However, the artefact still managed to bring about a ***learning*** experience in the players. This conclusion was derived from performing a comparison of the results obtained from a pre-test questionnaire and an identical post-test questionnaire. The post-test questionnaire was provided to the participants after they had completed the pre-test questionnaire and had interacted with the game-based artefact. Comparison of the results indicated that 60% of the participants achieved a ***learning*** experience from the game play, 20% experienced no ***learning***, and another 20% had a decline in their scores.

Section 7.3.3 discussed the *quality* aspects of the game-based artefact developed in this study. The artefact was evaluated according to three criteria, which are ***validity***, ***practicality***, and ***impact*** potential. ***Validity*** refers to the unique qualities of the game-based artefact, ***practicality*** to the way the tool fits and contributes to the target setting, and ***impact potential*** to the potential change the game-based artefact can bring about to the user. A summary of the results from Table 7-7 indicated that from a ***validity*** perspective, the artefact was developed with unique qualities through novel tools and materials. However, there was room for improvement identified in terms of consistency in how the content was delivered to the user. From the ***practicality*** perspective, the game-based artefact was practical to play but could be improved in terms of instrumentality by providing more information to the user at the start and during the game-play. From ***an impact potential*** perspective, the materials used in the game-based artefact were sufficient for the platform it was developed for and was able to impact the users by providing them with the information related to social engineering as intended. However, from the feedback obtained from the users, the quality in the materials used could have been improved, which may have provided a greater impact potential.

Chapter 8 will conclude this study by indicating whether the objectives of this study have been addressed. It will also discuss the reporting of this study, the study limitations, and future work that can stem from this study. A reflection from the researcher's point of view and final conclusion on the study will also be provided.

CHAPTER 8: CONCLUSION

8.1 Introduction

The primary objective of this study was to design and develop an artefact that can be used to raise awareness about social engineering attacks among administrative staff in medium to large organisations. This chapter will support the primary objective by concluding on the study through reflection. It will describe the research objectives that were initially set out in this study, as well as how these objectives were addressed. Future research that can be performed in relation to design science research and social engineering is also discussed.

The research component of this study was structured according to the DSRM process model by Peffers *et al.* (2007:54). Figure 8-1 illustrates the six activities of the DSRM process model.

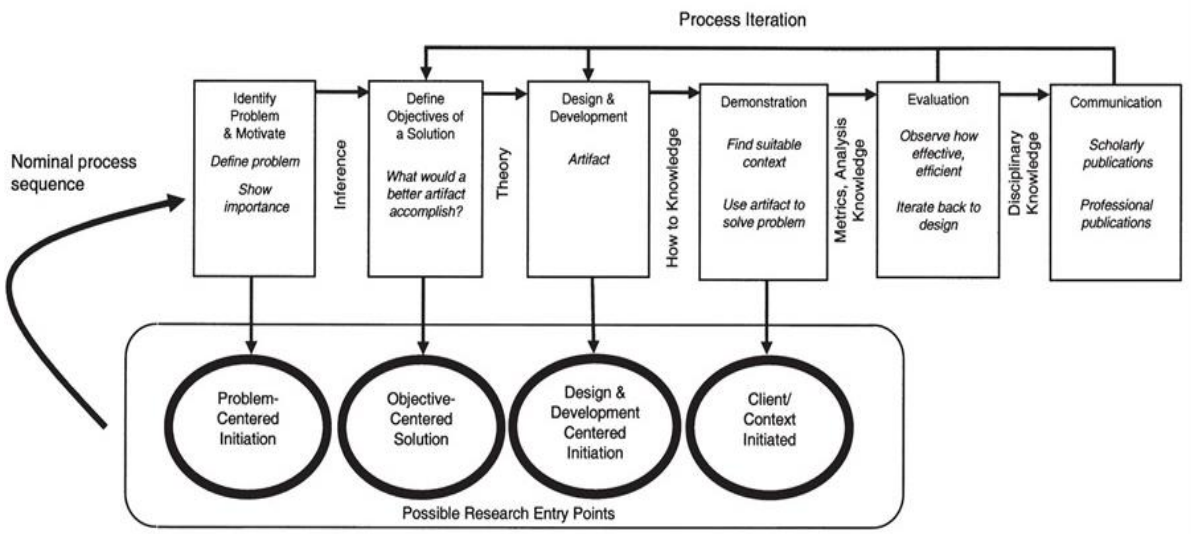


Figure 8-1: Design science research methodology (DSRM) process model (Peffers *et al.*, 2007:54)

The six activities, as they relate to the structure of this study, are:

1. **Problem identification and motivation:** The research problem was identified in Chapter 1 of this study, which was that administrative staff in medium to large organisations were vulnerable targets of social engineering attacks and lacked awareness of these attacks. This problem identification motivated the need for developing an artefact that could address the problem.

2. **Objectives of a solution:** The objective of the solution that would be developed in this study was defined in Chapter 1. To address the problem (defined in Section 1.3.1), the objectives (defined Section 1.3.2) were divided into the primary and secondary objectives. The secondary objectives supported the primary objective by describing the theoretical and empirical objectives that needed to be addressed. The theoretical objectives were addressed by the literature review. The literature also guided the approach followed in the empirical objectives by providing context. The understanding gained in the literature review guided the development of the solution. The objective was to develop a game-based artefact that could be used to address the problem identified in step 1 (problem identification and motivation). The literature relevant to the study were covered in Chapters 2 and 3.

3. **Design and development:** A novel artefact was developed in Chapters 4 through 6 using the design science research cycles by Hevner (2007:2). Design science research promotes a shared understanding of what constitutes a suitable artefact design based on the literature review. The theoretical objectives provided the literature for the design and development process. The empirical objectives described the design and development of the artefact.

4. **Demonstration:** The artefact was iteratively developed and demonstrated to participants in Chapters 5 and 6. Chapter 5 described the development of the conceptual artefact and conceptual prototype, which was iteratively demonstrated to the design experts (from academia) and participants (from academia) over two participatory design workshops (workshops 1 and 2). Chapter 6 described the development of the working prototype, which was also iteratively developed with the design experts (from academia) and demonstrated to the participants (from industry) in a participatory design workshop (workshop 3). The feedback received from the design experts and participants fed into the design and development process of the artefact until a suitable artefact was developed for the summative evaluation and testing phase (in Chapter 7).

5. **Evaluation:** The artefact was evaluated through summative evaluation and testing in Chapter 7 to determine whether it addressed the problem identified in step 1 (problem identification and motivation). It was also tested for *quality* against an artefact quality evaluation criteria as also described in Chapter 7. The summative evaluation and testing occurred in the form of a ***reaction*** and ***learning*** evaluation. In the ***reaction*** evaluation, all the participants (from academia and industry) who were involved in the design and development of the artefact participated in the evaluation. In the ***learning*** evaluation, a new set of participants (from industry) were involved. The results from the ***reaction*** evaluation were depicted in Section 7.3.1 and ***learning*** evaluation in Section 7.3.2. The *quality* evaluation occurred in the form of an evaluation against a set of criteria which aimed to evaluate the ***validity***, ***practicality***, and

impact potential of the developed game-based artefact. The quality evaluation of the artefact was discussed in Section 7.3.3.

6. **Communication**: The findings and reflection from the study are communicated in this chapter (Chapter 8).

Reflecting on this study, the research problem and primary objective were introduced in Chapter 1. The concepts central to the study were also discussed, which led to the literature review describing these central themes over Chapters 2 and 3.

Four research paradigms that are often used in computer science and information systems research and their applicable research methods, were discussed in the second chapter (in Section 2.2). This led to the study being grounded in the design science research paradigm (Section 2.5) discussed by Hevner (2007:2), as it aimed to develop a novel artefact that could be used to solve a real-world problem. Cyber-security was discussed in Chapter 3 in the form of a literature review. The section discussed cyber-security in general, and narrowed down to focus on social engineering as the central theme of this research in the field of cyber-security. A total of ten social engineering issues were identified (in Section 3.2.4) as being the most prevalent in the studies by Conteh and Schmick (2016) and Krombholz *et al.* (2015:116). A novel artefact aimed to address these social engineering issues. The novel artefact was developed (in Chapters 4 to7) in the form of a game-based artefact, the development of which was based on findings from the literature, guidance from design requirements identified from the research participants, and guidance from the design experts in academia.

Chapter 4 discussed the approach that was followed in developing the game-based artefact. This approach was grounded in the design science research cycles by Hevner (2007:2). Chapters 5 to 7 described the process of developing the game-based artefact, where the development activities were divided into the pre-, mid-, and post-artefact development activities. Pre-artefact development activities (Chapter 5) were the activities that occurred before the prototype was developed, which aimed to produce a conceptual artefact design as a mood board and storyboard; mid-artefact development activities (Chapter 6) were the activities that occurred as the working prototype was developed, which aimed to produce a working prototype; and the post-artefact development activities (Chapter 7) occurred after the artefact had been developed, where the usable prototype was evaluated through a summative evaluation and testing approach, which aimed to evaluate how the participants felt about the final design of the artefact and whether the artefact was able to address its primary objective of raising social engineering awareness.

In this chapter, Section 8.2 reflects on the research objectives that were set out at the beginning of the study, and how the work performed addressed these objectives. Section 8.3 reflects the reporting of this design science research study, which follows the reporting style of research by Mckenney and van den Akker (2005:41). The reporting approach provides the basis for reporting on the *quality* aspects of the artefact design. It also provides the basis for reporting on the artefact development and its evaluation. The design science research checklist by Hevner and Chatterjee (2010a:20) provides a checklist to confirm whether the outcomes of the DSR study have been communicated and is discussed in Section 8.4. The study limitations and future work are also discussed in Section 8.5, indicating the variables that limited the output of this study and what can be done to overcome these limitations in future work. The reflection and conclusion on the study are discussed in the final section (Section 8.6) of this chapter. The section describes the contributions this study has made to the research body of knowledge and any concluding thoughts about the study that could potentially be meaningful contributions.

8.2 Research objectives addressed

This section discusses how this study addressed the primary objective and secondary objectives, which were set out at the beginning of the study. The secondary objectives were divided into theoretical and empirical objectives.

8.2.1 Primary objective addressed by the study

The primary objective of this study was to design and develop an artefact that could be used to raise awareness about social engineering attacks among administrative staff in medium to large organisations. The primary objective of this study was addressed through the use of design science research as a research paradigm for developing a novel artefact. The game-based artefact allows players to learn about social engineering attacks through a series of challenges that require the player to make cognitive decisions, thereby allowing a learning experience to be incited. This ***learning*** experience incited by the artefact was tested using a pre- and post-test questionnaire, which was adapted from the questionnaire design by Jerry Chih-Yuan *et al.* (2017:48). The ***reaction*** evaluation of the artefact was in the form of an open-ended questionnaire. The open-ended questionnaire was structured as playtest questions, which were adapted from the work by Patton (2017) and Anonymous (2020). The two types of questionnaires for the ***learning*** and ***reaction*** evaluation were presented to the participants. The ***learning*** evaluation (discussed in Section 7.3.2) assessed the learning experience achieved by the participants when interacting with the artefact, and the ***reaction*** evaluation (discussed ion Section 7.3.1) evaluated their impressions and how they felt about the artefact. All of the participants who participated in the ***learning*** evaluation were administrative staff from a medium to large

organisation. The results from the ***learning*** evaluation indicated that 60% of the participants achieved a learning experience. The ***reaction*** evaluation indicated that the participants appreciated the simplicity in the gameplay and the platform being suitable for the purpose the game was designed. Even though the game was considered simple to play, the participants indicated that the main issue that made the gameplay difficult was that the heat maps on the images, which provide the interaction functionality, were not clearly distinguishable, making it difficult to manoeuvre in the game. Further design issues were identified and discussed in Section 7.3.1.2, and are noted as possible developments for future work.

From the results in Sections 7.3.1 and 7.3.2, it can be concluded that it was possible to develop an artefact that can be used raise awareness about social engineering attacks on administrative staff within medium to large organisations. The study limitations discussed in Section 8.5 indicate future work for possible extension of the research.

8.2.2 Secondary objectives addressed by the study

In order to address the primary objective, the theoretical and empirical objectives tabulated in Table 8-1 needed to be addressed. Table 8-1 describes how the study addressed these theoretical and empirical objectives. The objectives are structured according to the design science research methodology (DSRM) process model phases by Peffers *et al.* (2007:54).

Table 8-1: An outline of how the study addressed the theoretical and empirical objectives

DSR process	Description	How the objective is addressed by the study
Problem identification and motivation	**Theoretical objectives**	
	To identify the research problem.	The research problem was identified in the literature and is described in Section 1.3.1. The research problem was that social engineering attacks targeted at administrators are a threat to medium to large organisations.
	To motivate the process for conducting the research.	Design science research was identified in Section 1.2.3 as a suitable paradigm for artefact development. The research process for this study follows the DSRM process model by Peffers *et al.* (2007:54). The cyclical approach to design science research by Hevner (2007:2) was used to facilitate the design of the artefact.
	To determine the required fields of research to inform a solution for the research problem.	The fields of research identified for this study related to cyber-security, social engineering, and design science research. Cyber-security is key to the study. This is

DSR process	Description	How the objective is addressed by the study
		because social engineering is a subset of the main issues in cyber-security as defined in the literature. Design science research is the research paradigm suitable to guide this type of study.
Objectives of a solution	**Theoretical objectives** To create a shared understanding of design science research.	Four research paradigms were discussed in Section 2.2. Design science research was positioned in Section 2.2.5 as the preferred research paradigm for the study. Design science research was discussed in detail in Section 2.4.
	To understand the concepts of cyber-security and the area of social engineering within cyber-security.	Cyber-security was discussed in the literature in Section 3.2, with a key focus on social engineering in Section 3.2.4. Social engineering awareness was the key objective the solution needed to address.
	To identify what artefacts are available to raise cyber-security and social engineering awareness in particular.	Section 3.2.5 provided an overview of artefacts available to raise awareness on cyber-security issues, mainly social engineering awareness in particular. The artefacts identified in the literature included a memo, key chain, poster, slideshow presentation, as well as game-based delivery methods. This study focuses on game-based delivery methods to raise social engineering awareness.
	Empirical objectives Present findings from the literature in a participatory design workshop.	The findings from literature, in relation to the games available, were presented in a participatory design workshop.
	Analyse the feedback received from the requirements gathered during the participatory design workshops.	The feedback gathered from the participants during the participatory design workshops was analysed using open coding to identify themes in the data.
	Develop and present a conceptual design as a solution to the problem that is based on the requirements gathered from the target users.	The themes were used to guide the development of the conceptual artefact.
Design and development	**Theoretical objective** To form a conceptual link between design science research and the analysed feedback obtained from the requirements analysis.	The design science research cycles methodology by Hevner (2007:2) was used to guide the initial development of the artefact in conjunction with the feedback received from the requirements analysis.

DSR process	Description	How the objective is addressed by the study
	Empirical objectives To design and develop an artefact that meets the design and functionality requirements obtained from the requirements analysis.	An artefact was designed using requirements gathered from participants in participatory design workshops. The development of the artefact was performed using tools that were suitable based on the design requirements (see Sections 5.2.1 and 6.3.1 for a discussion on the tools used).
	To develop the artefact through an iterative approach until a usable prototype is reached.	The conceptual prototype was developed into a working prototype (see the iterative process described in Section 6.4.1), which was iteratively improved with design experts until a usable prototype was developed.
Demonstration	**Theoretical objectives** To explain how the requirements analysis and literature informed the design process through the use of artefact screenshots coupled with explanations.	The cyclical approach by Mckenney and van den Akker (2005:49) was used to present the artefact design process in the form of screenshots. This is depicted in Sections 5.3.1 and 6.4.1, which describe the iterative artefact design and development process from its conceptual design, to the prototype design using the feedback received from the participants and design experts. The design cycles by Hevner (2007:2) guide the process for the development of the artefact. The literature, which grounds the development process, is discussed in Section 4.1, which plans the approach for developing the artefact. The artefact development process is described in Section 5.4.1 and Section 6.5.1, respectively.
	Empirical objectives To demonstrate the artefact to the target audience.	The artefact was verbally presented to the target audience in two of the three participatory design workshops (workshops performed in Sections 5.3.1.1 and 5.3.1.4). The artefact was also provided to the participants for interaction in the third workshop for design feedback (workshop performed in Section 6.4.1.3). The artefact was finally provided to all the participants for interaction during the reaction and learning evaluations (Sections 7.3.1 and 7.3.2).
	To continuously evaluate the results obtained from the iterative demonstration of the artefact and determine any notable responses	The results from the iterative demonstration of the artefact during the workshops and design expert feedback sessions were evaluated and used to develop the working

DSR process	Description	How the objective is addressed by the study
	for future research at the end of the development prototype.	prototype. The iterative evaluations continued until a usable prototype design was reached.
Evaluation	**Theoretical objective** To determine a suitable reporting method for the feedback received from the summative evaluation and testing of the artefact.	The reporting on the evaluation of the artefact was discussed in Section 7.3 where two levels of the four-level evaluation by Petri and von Wangenheim (2016:995) were used to report on the feedback received from the participants.
	Empirical objectives To conduct a reaction evaluation with participants from the target audience as part of the evaluation of the artefact.	The developed artefact was presented to the participants as part of the reaction evaluation (Section 7.3.1.1). The reaction evaluation occurred as an open-ended gameplay questionnaire.
	To conduct a learning evaluation with participants from the target audience as part of the evaluation of the artefact.	The developed artefact was presented to the participants as part of the learning evaluation (Section 7.3.2.1). The learning evaluation occurred as pre- and post-test questionnaires.
	To analyse the feedback obtained from the reaction evaluation using qualitative data analysis techniques.	The artefact was evaluated by the participants in a reaction evaluation to determine whether it addressed the design requirements that were identified throughout the participatory design workshops. The results were qualitatively analysed using open coding to identify themes in the collected data (Section 7.3.1.2).
	To analyse the feedback obtained from the learning evaluation using quantitative data analysis techniques.	The artefact was evaluated by the participants in a learning evaluation to determine whether it addressed the learning objective as set out in the primary objective of the study. The results were quantitatively analysed through numerical comparison of the results of the pre- and post-test questionnaires (Section 7.3.2.2).
	To evaluate the quality of the artefact against a quality evaluation criteria.	The artefact was evaluated for quality in Section 7.3.3 using the artefact quality evaluation criteria by Mckenney and van den Akker (2005:48).
Communication	**Theoretical objectives** To communicate the design science research approach followed developing an artefact for raising social engineering	The design science research approach used to develop the artefact was discussed in Section 2.5. This is reported on in Section 8.3.

DSR process	Description	How the objective is addressed by the study
	awareness among administrative staff.	
	To communicate limitations within the context of the study by reflecting on restrictions of the research.	The limitations of the study are discussed in Section 8.5.
	To communicate future research within the context of the study by reflecting on recommendations for further improvement of the artefact.	Future work to extend this type of research is discussed in Section 8.5 with a reflection on this research discussed in Section 8.6.

8.3 Reporting on developing an artefact for raising social engineering awareness among administrative staff

The reporting of this design science research study follows a similar approach to that of Mckenney and van den Akker (2005) in their evaluation of the CASCADE-SEA program. An introduction to this approach was discussed in Section 2.5.4. Figure 8-2 is an adaptation of the research cycles by Mckenney and van den Akker (2005:49), and depicts the reporting approach as it relates to this study, which is cyclical in nature. Table 8-3 provides a summary overview of the number of participants involved in each of the cycle circuits (iterations). Each cycle is composed of multiple circuits, which essentially represent iterations that have activities. The activities are depicted as strategies in the table. It is best that Figure 8-2 is read in conjunction with Table 8-3 as Figure 8-2 summarises the cycles of Table 8-3. Table 8-2 is a legend for Table 8-3. The research cycles were performed over three phases, which were (1) the needs and context analysis; (2) the design, development, and formative evaluation of the prototype; and (3) the summative evaluation and testing of the prototype. These three phases, which summarise the approach of this study, are discussed.

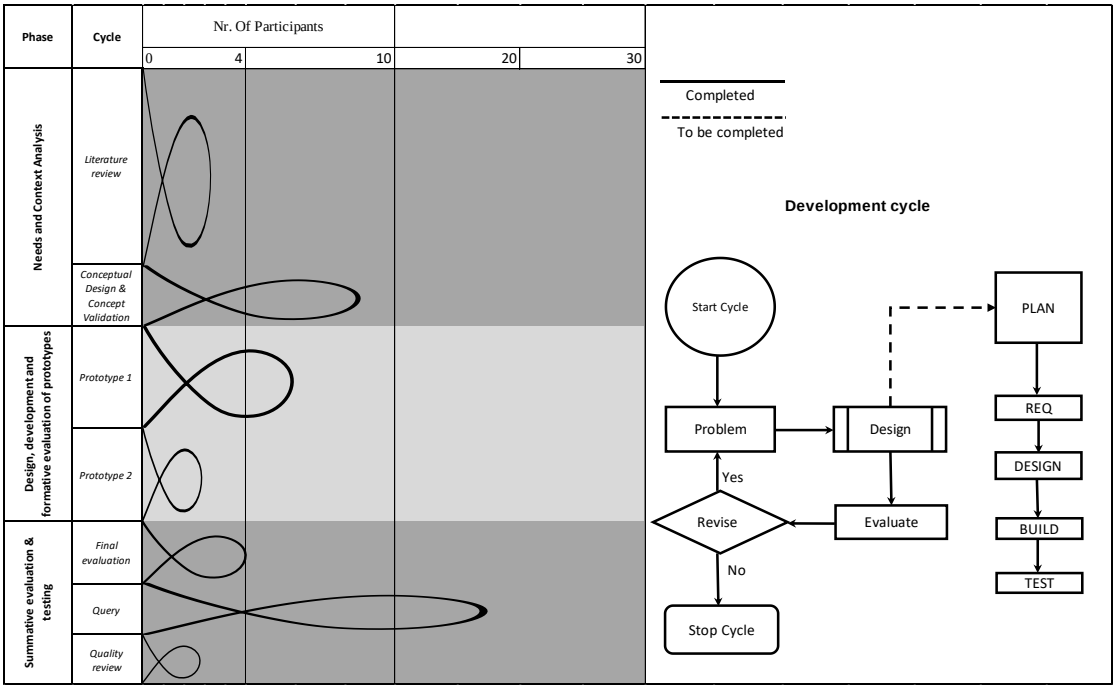


Figure 8-2: Research cycles by Mckenney and van den Akker (2005:49) for reporting this study

Table 8-2: Description of the legend depicted in Table 8-3

Legend item	Description
Strategies (strategies used in the cycle)	
RE=Reaction evaluation	An evaluation that aims to determine how a participant feels about the artefact.
LE=Learning evaluation	An evaluation that aims to determine whether there is a learning experience in the participant using the artefact.
AD=Artefact development	Time spent developing the artefact by the developer.
EA=Expert appraisal	Time spent by an expert performing as assessment of a circuit component.
ME= Micro evaluation	An evaluation case at a particular circuit.
TO= Try-out	Testing of the artefact by a user.
Users (users involved in the circuit)	
AIP=Academic institution participants	Participants from an academic institution who provide design inputs.
CIP=Corporate institution participants	Participants from a corporate institution who provide design inputs.
Experts (experts involved in the circuit)	
DSRE=Design science research experts	Design science research experts (from academia) who provide expert feedback at a particular circuit.

Legend item	Description
DA=Design artist	A design artist who provides expert feedback on the design elements at a particular circuit.
CSE=Cyber security expert	A cyber-security expert who provides expert feedback on cyber-security issues at a particular circuit.

Table 8-3: Overview of the strategies used over seven cycles consisting of 22 circuits until the completion of the summative evaluation and testing of the artefact

Phase	Cycle	Circuit	Strategy						Participants					#
									Users		Experts			
			AD	*EA*	*ME*	*TO*	*RE*	*LE*	*AIP*	*CIP*	*DSRE*	*DA*	*CSE*	
Needs and context analysis	*Literature review*	1		■							■			1
		2		■							■			2
		3		■							■			2
		4		■							■			2
		5		■							■			2
		6		■							■			2
		7		■							■			2
		8			■								■	1
		9		■							■			2
	Conceptual design & concept validation	10	■								■			2
		11	■			■			■		■			6
		12	■		■						■	■		3
		13	■		■	■					■	■		3
		14	■		■	■			■		■			6
Design, development and formative evaluation of prototypes	*Prototype 1*	15	■	■							■			2
		16	■	■							■			2
		17			■	■				■				4
	Prototype 2	18	■	■							■			2
		19	■	■							■			2
summative evaluation & testing	*Final evaluation*	20					■		■	■		■		4
	Query	21						■		■				15
	Quality review	22			■						■			2
Totals:			**9**	**12**	**6**	**4**	**1**	**1**	**3**	**3**	**18**	**3**	**1**	**61**
Estimated total participants when corrected for those who participated more than once:														**27**

Legend: ■ =Strategies used ■ = Types of participants

Strategies: RE=Reaction Evaluation; LE=Learning Evaluation; AD=Artefact Development; EA=Expert Appraisal; ME=Micro Evaluation; TO=Try-out
Users: AIP=Academic Institution Participants; CIP=Corporate Institution Participants
Experts: DSRE=Design Science Research Experts; DA=Design Artist; CSE=Cyber Security Expert

This section describes the results depicted in Table 8-3. In the **needs and context analysis,** the following activities occurred:

- To summarise, the *literature review* cycle occurred over 9 circuits (iterations), which are mapped to Chapters 2 to 4. Circuits 1 to 7 were a literature review described in Chapter 2 and Chapter 3. Circuit 8 was a validation of the literature discussed in Chapter 3. Circuit 9 was the discussion of Chapter 4. Each of these circuit outcomes are expanded as follows:
    - *Circuits 1 to 7* (Chapters 2 and 3) were the literature discussion relating to the research methodologies and cyber-security. Two design science research experts (DSREs) from academia were involved in these circuits. Each circuit represented a formal contact session between the researcher and the DSREs. The strategy (approach) for the seven circuits were in the form of expert appraisals (EA) where formal feedback was received and applied to the documentation of the literature review. It is important to note that many other feedback discussions were held with the DSREs in the form of document reviews, but were not added to the circuits, as they were not face-to-face contact sessions.
    - *Circuit 8* (Chapter 3 literature validation) was a micro-evaluation (ME) by a cyber-security expert (CSE) from industry to validate the cyber-security literature discussed in Chapter 3. An ME differs from an EA in that an ME is an evaluation, which by definition is a determination of whether something passes or fails based on objective criteria, whereas an EA is an assessment that seeks to evaluate understanding. The feedback received from the CSE was used to validate whether the content discussed in Chapter 3 was factually correct.
    - *Circuit 9* (Chapter 4) was an EA by the two DSREs from academia to assess the content discussed in Chapter 4. The content in Chapter 4 related to the planning of the approach to designing, developing, and evaluating the artefact over Chapters 5 to 7. Chapter 4 was used as a guideline to develop the conceptual design and the working prototype and to map the evaluation of the artefact.

- To summarise, the *conceptual design and concept validation* cycle occurred over five circuits (circuits 10 to 14) and was mapped to the artefact design sections in Chapter 5 (as Sections 5.3.1.1 to 5.3.1.4). The sections discussed the following: Presentation design (Section 5.3.1.1), mood board 1 design (Section 5.3.1.2), mood board 2 design (Section 5.3.1.3), and conceptual prototype design and concept validation (Section 5.3.1.4). The circuit outcomes were as follows:
    - *Circuit 10* (Section 5.3.1.1) was a presentation design process with the two design science research experts (DSREs) in preparation of the participatory design workshop that would occur in circuit 11. The strategy (event) at circuit 10 was an

artefact development (AD) that aimed to develop the PowerPoint presentation that would be presented in circuit 11.

- *Circuit 11* (also Section 5.3.1.1) was a participatory design workshop consisting of six participants (four academic institute participants (AIPs) and the two DSREs). Two strategies (events) were performed, one as a try-out (TO) and the other as an artefact development (AD). The TO occurred in the form of a presentation to the participants and the AD was the development of the conceptual design (mood board 1) after the participatory design workshop. The design requirements gathered during the workshop were used in the AD process.
- *Circuit 12* (Section 5.3.1.2) was a micro-evaluation (ME) by the two DSREs and a design artist (DA). The ME evaluated the design of the conceptual design (mood board 1) as developed (during the AD strategy) in Circuit 11. The results from the ME would be used to develop an improved conceptual design (mood board 2) as an AD process for presentation in circuit 13.
- *Circuit 13* (Section 5.3.1.3) was another ME and TO by the two DSREs and a DA. Mood board 2 was evaluated (as an ME) and tested (as a TO). The results from the ME and TO were used to improve mood board 2 and to develop the conceptual prototype as an AD process. Both the improved mood board 2 and the conceptual prototype would be presented in a participatory design workshop in circuit 14.
- *Circuit 14* (Section 5.3.1.4) was a participatory design workshop consisting of the same six participants (four academic institute participants (AIPs) and the two DSREs) who were involved in circuit 11. Two strategies (events) were performed, one as a TO and the other as an ME. The TO occurred in the form of a presentation of the conceptual design (mood board 2) and the conceptual prototype to the participants and the ME in the participants evaluating the two artefact designs. The results gathered during the participatory design workshop were used in circuit 15 to develop the prototype artefact.

In the **design, development, and formative evaluation of prototypes,** the following activities occurred:

- To summarise, the *prototype 1* and *prototype 2* development cycles occurred over five circuits and are mapped to the sections in Chapter 6 (as Sections 6.4.1.1 to 6.4.1.5). The sections discussed the following: Prototype 1 development and expert feedback (Section 6.4.1.1), prototype 1 improvement and expert feedback (Section 6.4.1.2), prototype 1 improvement and workshop presentation (Section 6.4.1.3), prototype 2 development and expert feedback (Section 6.4.1.4), and prototype 2 improvement and finalisation (Section

6.4.1.5). The prototype 1 development occurred over three iterations (circuits) and prototype 2 over two iterations (circuits). The circuit outcomes are expanded as follows:

- *Circuit 15* (Section 6.4.1.1) was the development of prototype 1 as an artefact development (AD) strategy. The design requirements used to develop prototype 1 in this circuit were obtained from the participatory design workshop in circuit 14. The artefact was evaluated as a micro-evaluation (ME) by the design science research experts (DSREs) for design improvement. The feedback was used to develop an improved prototype 1 in circuit 16.
- *Circuit 16* (Section 6.4.1.2) followed the same process as followed in circuit 15. It is the improvement of prototype 1 as an AD strategy. The design was evaluated by the DSREs as an ME strategy. The feedback from the ME was used to develop an improved prototype 1 as an AD strategy and present the improved prototype 1 as a participatory design workshop in circuit 17.
- *Circuit 17* (Section 6.4.1.3) was the presentation of prototype 1 to corporate institution participants (CIPs). The CIPs tried-out (TO) the prototype by physically interacting with it and providing feedback as an ME strategy. The feedback received from the ME was used to develop prototype 2 in circuit 18.
- *Circuit 18* (Section 6.4.1.4) followed a similar approach to circuit 15. It is the development of prototype 2 as an artefact AD strategy. The design requirements used to develop prototype 2 in this circuit were obtained from the participatory design workshop in circuit 17. The artefact was evaluated as an ME by the DSREs for design improvement. The feedback was used to develop an improved prototype 2 in circuit 19.
- *Circuit 19* (Section 6.4.1.5) followed a similar approach to circuit 16. It was the improvement of prototype 2 as an AD strategy. The design was evaluated by the DSREs as an ME strategy. The feedback received from the ME was used to develop an improved prototype 2 as an AD strategy. The improved prototype 2 was evaluated as a ***reaction*** evaluation (circuit 20), ***learning*** evaluation (circuit 21), and *quality* review (circuit 22) during the summative evaluation and testing phase.

In the **summative evaluation and testing,** the following activities occurred:

- To summarise, the *final evaluation*, *query* evaluation, and *quality review* cycles occurred over three circuits and are mapped to sections in Chapter 7 (as Sections 7.3.1, 7.3.2 and 7.3.3 respectively). The sections discussed the following: The ***reaction*** evaluation of the working prototype (Section 7.3.1), the ***learning*** evaluation of the working prototype

(Section 7.3.2) and the *quality* review of the prototype (Section 7.3.3). The working prototype is hereafter referred to as the game-based artefact. The circuit outcomes are expanded as follows:

- *Circuit 20* (Section 7.3.1) was the ***reaction*** evaluation (RE) of the game-based artefact (final prototype 2). It assessed how the participants felt about the design of the artefact. The RE occurred in the form of open coding on the feedback received from the participants. The feedback was obtained by presenting the participants with the artefact and a questionnaire containing open-ended questions (see Appendix O for open-ended questionnaire structure). The questions were based on questions generally asked during playtest feedback sessions and were based on the playtest questions by Patton (2017) and Anonymous (2020). The participants involved in the RE were three academic institution participants (AIPs) and one corporate institution participant (CIP). Due to the COVID-19 pandemic, the open-ended questionnaires were distributed using Google Forms. The data captured in forms was kept anonymous by not capturing any identifying information. The results from the qualitative analysis of the open-coded results were discussed in Section 7.3.1.2.
- *Circuit 21* (Section 7.3.2) is the ***learning*** evaluation (LE) of the game-based artefact (final prototype 2). It assessed whether the artefact brought about a learning experience in the participants. The LE occurred in the form of a pre- and post-test questionnaire (see Appendices N and O for the questionnaire structure), which were identical and presented to the participants before and after they interacted with the artefact. The structures of the pre- and post-test questionnaire were based on the study by Jerry Chih-Yuan *et al.* (2017:58). The questions depicted in the questionnaire were based on the six social engineering issues addressed in the game-based artefact (see Section 6.2 for contextual discussion on the social engineering issues depicted in the game-based artefact). The social engineering issues addressed by the artefact were an excerpt from the ten social engineering issues described in the literature (Section 3.2.4) by Conteh and Schmick (2016:32) and Krombholz *et al.* (2015:116). Due to the COVID-19 outbreak, it was also not possible to perform the ***learning*** evaluation as a workshop with the participants during the summative evaluation and testing. The questionnaires were therefore distributed using Google Forms, as it was a more suitable avenue for allowing a high volume of participants to easily capture their responses in the questionnaires. The questionnaire was completed by 15 CIPs. The results from the quantitative analysis of the questionnaire results were discussed in Section 7.3.2.2.

- *Circuit 22* (Section 7.3.3) is the *quality* review on the artefact. It assessed whether the artefact had been developed in such a way that it met the quality criteria as defined by Mckenney and van den Akker (2005:48). The criteria examined the artefact's ***validity***, ***practicality***, and ***impact potential***. A summary of the results from the criteria indicated that the artefact was designed to suitably address its main objective. However, certain design improvements were identified that could improve the overall user experience. From a ***validity*** perspective, some changes to the platform and user interface could be improved. From a ***practicality*** perspective, the artefact was practical enough in its use and consistent in its design; however, improvements such as increasing the amount of queues and tutorial were identified. The ***impact potential*** indicated that the materials used in the game-based artefact were sufficient for the platform it was developed for and was able to impact the users by providing them with the necessary knowledge related to social engineering attacks as intended.

Additionally depicted in Figure 8-2 was the development process of prototype 1 and prototype 2. It mapped to the **design, develop, and formative evaluation of prototypes** phase of Table 8-3. The development cycle depicted a *problem* identification, the identification of which lead to the *design* phase. The *design* phase was followed iteratively (from planning → gathering requirements → designing → building the artefact → then testing it) to develop the artefact until the design experts approved that the design was adequate for *evaluation* by the participants. The artefact was then *revised* to confirm whether the cycle should be repeated or could move to the next cycle. Sections 6.4.1.1 to 6.4.1.5 extensively discussed the working prototype design and development process.

The artefact was developed and evaluated over a total of 22 circuits and consisted of 27 unique participants. The participatory design approach is depicted in Appendix D. Four experts were involved, two of whom were design experts, one a cyber-security expert, and another was a design artist who provided expert guidance on the design elements of the artefact. Four participants (from Company A) provided design input that was used to develop a suitable artefact. The four participants all formed part of the ***reaction*** evaluation during the summative evaluation and testing of the developed artefact. An additional four target user participants (from Company B) also provided design input that was used to develop the artefact. Two of the four participants from Company B formed part of the target user participants and the remaining two were cyber-security professionals. Fifteen additional unique participants (from Company B) were part of the ***learning*** evaluation during the summative evaluation and testing.

The study is therefore concluded over a total of 61 strategy and participatory sessions (as depicted in Table 8-3), where 33 of the strategy sessions involved 9 artefact development sessions (AD), 12 expert appraisal sessions (EA), 6 micro-evaluation sessions (ME), 4 try-out sessions (TO), 1 ***reaction*** evaluation session (RE), and 1 ***learning*** evaluation session (LE). The remaining 28 participatory sessions consisted of 3 academic institute participant (AIPs) sessions, 3 corporate institute participant (CIP) sessions, 18 design science research expert (DSRE) sessions, 3 design artist (DA) sessions, and 1 cyber-security expert (CSE) session. The participant sessions were in the form of face-to-face contact sessions.

8.4 DSR checklist

Table 8-4 provides a checklist questionnaire that can be used to evaluate the success of a DSR study. It provides a list of questions that assess the progress on design research projects in order to ensure that the projects address important aspects of DSR studies (Hevner & Chatterjee, 2010a:19). The checklist questions are answered in context of this study and provide a checklist to confirm whether this study addressed the important aspects of DSR studies.

Table 8-4: Design science research checklist (Hevner & Chatterjee, 2010a:20)

Questions	Answers from the study
1. What is the research question (design requirements)?	Three research questions identified in this study were: Which type of artefact is suitable to raise social engineering awareness among administrative staff? How can an artefact be designed in a way that it can meet user acceptance requirements to raise awareness on social engineering? How can design science research be used to design an artefact to raise social engineering awareness among administrative staff? The design requirements were extracted from these research questions by providing secondary theoretical and empirical objectives which were structured according to the DSRM process model by Peffers *et al.* (2007:54).
2. What is the artefact? How is the artefact represented?	The artefact is a game-based prototype developed in the form of a storyboard structure using Twine 1.4.2 game development engine for functionality and Unity 2019.1.14 game development for the user interface. The artefact is playable online using a web browser and can be accessed at https://socios3c.online/. It is represented as a series of challenges and video tutorials that aim to incite a learning experience in the player.
3. What design processes (search heuristics) will be used to build the artefact?	The design processes that were used to guide the design and development of the artefact were the requirements gathered from the participants in the participatory design workshops, as well as the experience of the design experts who guided the design and development process. The design science research cycles by Hevner (2007:2), as described in Section 2.4.1.3, were used to guide the process of designing, developing, and evaluating the artefact. The artefact design and development process followed an agile development methodology which is iterative in nature and closely involved the users and developers throughout the development process.

Questions	Answers from the study
4. How are the artefact and the design processes grounded by the knowledge base? What, if any, theories support the artefact design and the design process?	The design science research cycles by Hevner (2007:2) were used as the artefact development framework. The cyclical approach by Mckenney and van den Akker (2005:49) was used to guide and report the development of the artefact. The cyclical approach depicted the process of identifying the needs and context analysis for developing the artefact, which was grounded in the literature. The cyclical approach also described the prototype design, development, and formative evaluation, as well as the summative evaluation and testing of the prototype artefact.
5. What evaluations are performed during the internal design cycles? What design improvements are identified during each design cycle?	Figure 8-2 depicted the development cycle used in the development of the prototype artefact. It was an adaptation of the cyclical approach described by Mckenney and van den Akker (2005:49). Testing was performed continuously with the design experts as well as the participants in participatory design workshops.
6. How is the artefact introduced into the application environment and how is it field tested? What metrics are used to demonstrate artefact utility and improvement over previous artefacts?	The artefact was introduced to the environment through a summative evaluation and testing approach. The summative evaluation and testing was performed with a variety of participants who fall within the target user group as a ***learning*** evaluation (see Section 7.3.2). The target user group participants as well as two cyber security professionals were involved in the ***reaction*** evaluation (see Section 7.3.1) of the artefact during summative evaluation and testing phase. The ***learning*** evaluation involved a pre- and post-test, which evaluates the utility of the artefact. The results from the pre- and post-test were compared and it was found that 60% of the participants who participated in the test had achieved a learning experience. The ***reaction*** evaluation was in the form of an open-ended questionnaire provided to the participants after they had interacted with the prototype. The aim of the ***reaction*** evaluation was to determine whether the artefact was designed in a way that it adequately catered to their requirements identified in the prior participatory design workshops. The results indicated that the artefact was usable, but had design issues that could be improved in future research. The artefact was evaluated for *quality* in Section 7.3.3 using the artefact *quality* evaluation criteria by Mckenney and van den Akker (2005:48). Quality criteria involved evaluating the artefact for its ***validity***, ***practicality***, and ***impact potential***.
7. What new knowledge is added to the knowledge base and in what form (e.g. peer-reviewed literature, meta-artefacts, new theory, new method)?	Additions to the research knowledge base were in the form of validations of the tools used to develop the prototype artefact. The tools used in each development stage were depicted in the rigor cycles of Chapters 5 to 7. A game-based artefact was also a contribution to the artefacts in the DSR knowledge base. A DSR approach to reporting on a Master of Science (MSc) dissertation was also an addition to the knowledge base. Further additions to the knowledge base were in the form of two conference papers, one was published in March 2020 which is titled '*Creating a conceptual design for a game-based artefact'* and was published in the proceedings of *EdMedia and Innovate Learning 2020 Online, Netherland, June 23-26, 2020*: URL: https://learntechlib.org/noaccesspresent/217373/ and the other paper is titled '*Raising social engineering awareness through gameplay'* which was submitted to the 19th World Conference on Mobile and Contextual Learning (mLearn) on August 1st, 2020 and was presented with the proceedings forthcoming. Proof of submission for the conference paper can be found in Appendix P.
8. Has the research question been	The three research questions identified in question 1 were addressed as follows:

Questions	Answers from the study
satisfactorily addressed?	The artefact that administrative staff were most comfortable with was a game-based artefact designed in the form of a story board style. The artefact had to be interactive and easily accessible from their desktop devices ideally through a platform such as a web browser; The artefact was tested and evaluated through a summative evaluation and testing approach. The summative evaluation and testing addressed the user acceptance test through the ***reaction*** level evaluation, which evaluated how the users felt about the artefact and whether it adequately addressed their design requirements. The ***learning*** level evaluation in the summative evaluation and testing of the artefact addressed the raising of social engineering awareness on the users portion of the research question; and The design science research paradigm was used to develop a functional prototype artefact that, when tested through a pre- and post-test questionnaire in a summative evaluation and testing approach, revealed that it was able to address the primary objective of the study, which was to raise awareness about social engineering issues.

8.5 Study limitations and future work

A limitation of this study was that the artefact could only be tested using two levels (***reaction*** and ***learning*** evaluation) of the four-level model for evaluating artefacts by Petri and von Wangenheim (2016:995). The ***reaction*** level evaluates how participants feel, whereas the ***learning*** level evaluates whether a learning experience has occurred. The *behaviour* level evaluates the degree to which the learning acquired can be transferred to the participant's job performance, i.e. whether the learning experienced by the participants has managed to change behaviour over an extended period. The *results* level evaluates the effect the learning has on the environment over time, i.e. it aims to determine whether the learning has had any influence on the environment over a period of time. As the focus of this study was only on the initial development of the game-based artefact using a DSR approach, the *behavioural* and *results* levels from the four-level model can only be implemented and formally evaluated once the design of the artefact has been approved for use. The time required to evaluate these two levels was not available in this study and this therefore servers as a limitation to this study.

A further limitation was that due to time limitations, it was not possible to develop and simultaneously test a narrative/storyboard game-based artefact (as developed in this study) and a 3D game-based artefact (which could be developed if more time and development skills are available). It would be of value to test and evaluate both these artefacts together, for both the ***learning*** and ***reaction*** evaluation, as some of the participants requested a 3D artefact design. This would potentially provide different responses from the participants for the ***reaction*** evaluation and could potentially enhance the results of the ***learning*** evaluation.

Due to the COVID-19 pandemic, it was also not possible to perform the ***learning*** evaluation (pre- and post-test) and ***reaction*** evaluation (open-ended questionnaire) as a participatory design workshop with the participants during the summative evaluation and testing. The workshop would have potentially enabled a richer feedback to be provided by the participants on the design of the artefact and how the learning experience was achieved.

Future work would be that the artefact could be expanded to include more automation and, if possible, artificial intelligence (AI) to make the artefact less predictable. The artefact's design could be enhanced to a 3D game-based artefact which would be visually appealing for some participants. The artefact can also be developed and tested to cater for target user participants from rural areas as the challenges faced by participants working in urbanised and better connected areas are different from those in rural areas. People from rural areas are known to be more vulnerable to social engineering attacks given their limited exposure to technology and awareness regarding cyber risks. Additionally, research can build on these observations by developing an artefact that is cross platform (usable on any device). The artefact can aslo be tested through simulation, by potentially performing a 'real-world' social engineering attack on the participants, introducing them to the artefact to bring about a learning experience, and then re-performing the social engineering attack to determine whether the artefact had indeed brought about a learning experience in the participants. Consideration can also be made (given enough time and resources) to test the artefact over a longer period with the participants. This can be achieved by performing continuous and controlled social engineering attacks on the participants that are shortly followed by an awareness campaign. This would measure the behavioural changes in the participants, thereby satisfying the behaviour evaluation level of the four-level evaluation model by Petri and von Wangenheim (2016:995). The ethical implications of this approach however would need to be clearly defined and understood to ensure that the study is performed in an ethically controlled environment.

8.6 Reflection and conclusion

The aim of this study was to design and develop an artefact that could be used to raise awareness about social engineering attacks among administrative staff in medium to large organisations. It was achieved by reviewing the existing literature to achieve a shared understanding of research methodologies and cyber-security. Artefacts already existing in the research body of knowledge, and design science research was used to inform the development of a novel artefact. Knowledge contributions were made to the research body of knowledge in the form of two conference papers. The first paper was on creating conceptual artefacts for games, which was titled *Creating a conceptual design for a game-based artefact* and was published in the proceedings of *EdMedia and Innovate Learning 2020 Online, Netherland, June 23-26, 2020*: URL:

https://learntechlib.org/noaccesspresent/217373/. The paper is an excerpt from this study and provides researchers with a strategy for creating a conceptual design for a game-based artefact as well as how to report on the design process.

The other paper was titled '*Raising social engineering awareness through gameplay*' which was submitted to the 19th World Conference on Mobile and Contextual Learning (mLearn) on August 1st, 2020 and was presented with the proceedings forthcoming. Proof of submission for the second conference paper can be found in Appendix P. The paper presents a game-based artefact that can be used to raise social engineering awareness among administrative target users. A case study is presented in the paper, via a design science research model, which includes discussion on the processes followed for creating a conceptual design, a prototype, and evaluating the artefact.

Other contributions were in the form of validations of tools and processes that worked well during the design, development, and evaluation of the novel artefact.

The results from the artefact evaluation in Chapter 7 indicated that game-based artefacts could be used to raise awareness about social engineering issues for administrative staff in medium to large organisations. The results also indicated that game-based artefacts that are accessible over the web are more preferred for a digitally connected society that prefers to be able to access resources from any location. Video tutorials were also identified to be a suitable avenue for raising awareness during gameplay.

A possible addition to representing research activities would be to improve the Mckenney and van den Akker (2005:51) research activities table by including the time spent on a circuit as an additional variable. As the table stands, it only indicates the circuits at each cycle with the number of participants involved, but does not indicate the time spent at the circuit. This would be valuable as it would depict the effort involved at each circuit.

Design science research has proven to be a useful approach to developing and reporting on artefact creation. Design science research facilitates the iterative development of novel artefacts and provides the ability to closely involve participants for which the artefact would be developed. It also provides the guidelines for developing useful and acceptable artefacts.

The key personal takeaways from using DSR in this study was that DSR is a rigorous research process that guides the development of an artefact in a scientific manner. DSR supports agile software development methodologies which enables the artefacts to be developed within a short turnaround time. The agile methodology also closely involves the developers and the users, allowing design requirements to be quickly gathered, applied, and reviewed. This allows the

artefact to be built in a way that it can adequately satisfy and cater to the user design requirements. The DSR methodology also enables the artefact design and research outcomes to be adequately captured and documented, thereby adding to the research body of knowledge. The quality of the artefact design and development was greatly improved under guidance of the DSR methodology.

REFERENCES

Ab Razak, M.F., Anuar, N.B., Salleh, R. & Firdaus, A. 2016. The rise of "malware": Bibliometric analysis of malware study. *Journal of Network and Computer Applications*, 75:58-76.

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

Al-Khouri, A.M.S. 2007. Strategic and large scale government IT projects management: innovation report. University of Warwick.

Al-Rabiaah, S. 2018. *The "stuxnet" virus of 2010 as an example of a "APT" and its "recent" variances*. Paper presented at the National Computer Conference (NCC), Riyadh, Saudi Arabia.

Aldawood, H. & Skinner, G. 2018. Educating and raising awareness on cyber security social engineering: A literature review. (In: International Conference on Teaching, Assessment, and Learning for Engineering (TALE) organised by Wollongong, NSW, Australia: IEEE. p. 62).

Anderson, G.J. 1990. *Fundamentals of educational research*: London, New York: Falmer, 1990.

Anonymous. 2008. Master of Security. https://www.kongregate.com/games/gmentat/master-of-security Date of access: 11 February 2020.

Anonymous. 2014. 6 Methods of data collection and analysis. www.open.edu/openlearncreate/mod/resource/view.php?id=52658 Date of access: 01 October 2018.

Anonymous. 2016. South African university website hacked by Anonymous. https://mybroadband.co.za/news/security/165004-south-african-university-website-hacked-by-anonymous.html Date of access: 19 February 2017.

Anonymous. 2019. Advanced persistent threat (APT). https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/ Date of access: 31 May 2019.

Anonymous. 2020. Playtesting feedback form. https://www.kathleenmercury.com/uploads/2/2/7/4/22743302/game_salute_playtest_form_-_fillable-4.pdf Date of access: 28 April 2018.

Anthony, L., Prasad, S., Hurst, A. & Kuber, R. 2012. A participatory design workshop on accessible apps and games with students with learning differences. *ACM SIGACCESS Conference on Computers & Accessibility*:253-254.

Barbieri, D., Cardellini, V. & Filippone, S. 2014. Exhaustive key search on clusters of gpus. (In: 2014 IEEE International Parallel & Distributed Processing Symposium Workshops organised by: IEEE. p. 1160-1168).

Barrett, N. 2003. Penetration testing and social engineering: Hacking the weakest link. *Information Security Technical Report*, 8(4):56-64.

Baskerville, R.L., Kaul, M. & Storey, V.C. 2015. Genres of inquiry in design-science research: Justification and evaluation of knowledge production. *MIS Quarterly*, 39(3):541-549.

Baskerville, R.L. & Pries-Heje, J. 2019. Projectability in Design Science Research. *J. Inf. Technol. Theory Appl.*, 20(1):3.

Bendovschi, A. 2015. Cyber-attacks: Trends, patterns and security countermeasures. *Procedia Economics and Finance*, 28:24-31.

Bergstedt, J. 2015. Learning facilitators' perspectives of supporting learners with disabilities in mainstream classrooms. Stellenbosch: Stellenbosch University.

Berinato, S. 2002. Cybersecurity: The truth about cyberterrorism. https://www.cio.com/article/2440933/cybersecurity---the-truth-about-cyberterrorism.html Date of access: 11 February 2020.

Biancotti, C. 2017. The price of cyber (in) security: Evidence from the italian private sector. *Bank of Italy Occasional Paper,* (407).

Biswas, A., Sen, S. & Ray, K. 2019. Reliability assessment of pre-post test questionnaire on the impact of a daylong clinical pharmacology workshop among medical professionals. *Asian Journal of Medical Sciences*, 10(6):93-97.

Bowen, G.A. 2009. Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2):27-40.

Breda, F., Barbosa, H. & Morais, T. 2017. Social engineering and cyber security. (In: International Technology, Education and Development Conference organised by: ISACA and RSA.

Brenner, S.W. 2006. Cybercrime, cyberterrorism and cyberwarfare. *Revue Internationale de Droit Pénal*, 77(3):453-471.

Brom, C., Buchtová, M., Šisler, V., Děchtěrenko, F., Palme, R. & Glenk, L.M. 2014. Flow, social interaction anxiety and salivary cortisol responses in serious games: A quasi-experimental study. *Computers & Education*, 79:69-100.

Bullée, J.-W.H., Montoya, L., Pieters, W., Junger, M. & Hartel, P.H. 2015. The persuasion and security awareness experiment: Reducing the success of social engineering attacks. *Journal of Experimental Criminology*, 11(1):97-115.

Carney, I. & Department of Defense. 2010. CyberProtect. http://sgschallenge.com/cyber-protect/ Date of access: 22 April 2019.

Carroll, J.M. & Rosson, M.B. 2007. Participatory design in community informatics. *Design Studies*, 28(3):243-261.

Chu, H. & Ke, Q. 2017. Research methods: What's in the name? *Library and Information Science Research*, 39:284-294.

Ciancioso, R., Budhwa, D. & Hayajneh, T. 2018. A framework for zero day exploit detection and containment. (In: Elsevier, B.V. organised by: Institute of Electrical and Electronics Engineers Inc. (IEEE). p. 663-668).

Cohen, L., Manion, L. & Morrison, K. 2007. Research methods in education: London: Routledge.

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.

Cone, B.D., Thompson, M.F., Irvine, C.E. & Nguyen, T.D. 2006. Cyber security training and awareness through game play. *International Federation for Information Processing (IFIP)*, 201:431-436.

Conteh, N.Y. & Schmick, P.J. 2016. Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23):31-38.

Cordeiro, L., Barreto, R., Barcelos, R., Oliveira, M., Lucena, V. & Maciel, P. 2007. Agile development methodology for embedded systems: A platform-based design approach. (In: 14th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems organised by: IEEE. p. 195-202).

Creswell, J.W. 1998. *Qualitative inquiry and research design: Choosing among five traditions*. Thousand Oaks, CA, US: Sage Publications, Inc.

Creswell, J.W. 2014. *Research design: Qualitative, quantitative, and mixed methods approaches*: Los Angeles, Calif.: SAGE, [2014]. 4th ed.

Croock, G. 2016. An Africa Perspective: Cyber Threats, Security and Data Protection. https://www.bdo.co.za/en-za/insights/2016/cyber/an-africa-perspective-cyber-threats-security-and-data-protection Date of access: 18 May 2017.

Dilshad, R.M. & Latif, M.I. 2013. Focus group interview as a tool for qualitative research: An analysis. *Pakistan Journal of Social Sciences (PJSS)*, 33(1):191-198.

Doody, O., Slevin, E. & Taggart, L. 2013. Focus group interviews. Part 3: Analysis. *British Journal of Nursing*, 22(5):266-269.

Fahl, S., Harbach, M., Muders, T., Baumgärtner, L., Freisleben, B. & Smith, M. 2012. Why eve and mallory love android: An analysis of android SSL (in) security. (In: Proceedings of the 2012 ACM conference on Computer and communications security organised by: ACM. p. 50-61).

Fatima, S. & Naima, K. 2019. Social engineering attacks: A survey. *Future Internet*(4):89.

Furnell, S. & Vasileiou, I. 2017. Security education and awareness: Just let them burn? *Network Security*, 2017(12):5-9.

Gallegos-Segovia, P.L., Bravo-Torres, J.F., Larios-Rosillo, V.M., Vintimilla-Tapia, P.E., Yuquilima-Albarado, I.F. & Jara-Saltos, J.D. 2017. Social engineering as an attack vector for ransomware. (In: (CHILECON) Conference on Electrical, Electronics Engineering, Information and Communication Technologies organised by: IEEE. p. 1-6).

Goede, R. 2004. *A framework for the explicit use of specific systems thinking methodologies in data-driven decision support system development*: 2004.

Golafshani, N. 2003. Understanding reliability and validity in qualitative research. *The Qualitative Report*, 8(4):597-606.

Gordon, S. & Ford, R. 2006. On the definition and classification of cybercrime. *Journal in Computer Virology*, 2(1):13-20.

Granger, S. 2001. Social engineering fundamentals, part i: Hacker tactics. *Security Focus, December*, 18.

Green, M. & Smith, M. 2016. Developers are not the enemy!: The need for usable security apis. *IEEE Security & Privacy*, 14(5):40-46.

Gregor, S. & Hevner, A.R. 2013. Positioning and presenting design science research for maximum impact. *MIS Quarterly*, 37(2):337-355.

Gu, G., Zhang, J., Lee, W. & Perdisci, R. 2008. *Botminer: Clustering analysis of network traffic for protocol- and structure-independent botnet detection*. Paper presented at the 17th USENIX Security Symposium. https://nwulib.nwu.ac.za/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edselc&AN=edselc.2-52.0-85075837457&site=eds-live Date of access: 18 October 2019.

Guba, E.G. & Lincoln, Y.S. 1994. Competing paradigms in qualitative research. *Handbook of Qualitative Research*, 2(163-194):105-117.

Harvey, L. 1990. *Critical social research*. Available from SCRIBD: https://www.scribd.com/document/106256623/Lee-Harvey-Critical-Social-Research. Date of access: 12 July 2020.

Hatfield, J.M. 2018. Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, 73:102-113.

Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W. & Spiegel, J. 2012. The law of cyber-attack. *California Law Review*, 100(4):817-885.

Healy, M. & Perry, C. 2000. Comprehensive criteria to judge validity and reliability of qualitative research within the realism paradigm. *Qualitative Market Research: An International Journal,* (3):118.

Heartfield, R. & Loukas, G. 2015. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, 48(3):1-39.

Hendrix, M., Al-Sherbaz, A. & Victoria, B. 2016. Game based cyber security training: are serious games suitable for cyber security training? *International Journal of Serious Games*, 3(1):53-61.

Herselman, M. & Warren, M. 2004. Cyber crime influencing businesses in South Africa. *Issues in Informing Science & Information Technology*, 1:253-266.

Hevner, A. & Chatterjee, S. 2010a. Design science research in information systems. Design research in information systems: Theory and practice. Boston, MA: Springer US. p. 9-22).

Hevner, A.R. 2007. A three cycle view of design science research. *Scandinavian Journal of Information Systems*, 19(2):4.

Hevner, A.R. & Chatterjee, S. 2010b. *Design research in information systems: theory and practice*: Springer.

Hevner, A.R., March, S.T., Park, J. & Ram, S. 2004. Design science in information systems research. *MIS Quarterly*, 28(1):75-105.

Heymann, R. & Greeff, J.J. 2018. *Designing and developing a narrative driven serious game for teaching information theory*. Paper presented at the 2018 IEEE Global Engineering Education Conference (EDUCON), 17-20 April 2018.

Hirschheim, R. & Klein, H.K. 1989. Four paradigms of information systems development. *Communications of the ACM*, 32(10):1199-1216.

Hoepfl, M.C. 1997. Choosing Qualitative Research: A Primer for Technology Education Researchers (Vol. 9. pp. 47-63): Journal of Technology Education.

Hox, J.J. & Boeije, H.R. 2005. Data collection, primary versus secondary. http://hdl.handle.net/1874/23634 Date of access: 18 July 2020.

Ivaturi, K. & Janczewski, L. 2011. A taxonomy for social engineering attacks. (In: International Conference on Information Resources Management organised by: Centre for Information Technology, Organizations, and People. p. 1-12).

Jagatic, T.N., Johnson, N.A., Jakobsson, M. & Menczer, F. 2007. Social phishing. *Communications of the ACM*, 50(10):94-100.

Jain, J. & Pal, P.R. 2017. A recent study over cyber security and its elements. *International Journal of Advanced Research in Computer Science*, 8(3):791-793.

Jansson, K. & Von Solms, R. 2011. Social engineering: Towards a holistic solution. (In: Proceedings of the South African Information Security Multi-Conference: Port Elizabeth, South Africa, 17-18 May 2010 organised by: Lulu. com. p. 23).

Jansson, K. & von Solms, R. 2013. Phishing for phishing awareness. *Behaviour & Information Technology*, 32(6):584-593.

Jerry Chih-Yuan, S., Cian-Yu, K., Huei-Tse, H. & Yu-Yan, L. 2017. Exploring learners' sequential behavioral patterns, flow experience, and learning performance in an anti-phishing educational game. *Journal of Educational Technology & Society*, 20(1):45-60.

John, M. 2001. Combining IS research methods: Towards a pluralist methodology. *Information Systems Research*, 12(3):240.

Kafol, C. & Bregar, A. 2017. Cyber security: Building a sustainable protection. *DAAAM International Scientific Book* 81-90.

Khaled, R. & Vasalou, A. 2014. Bridging serious games and participatory design. *International Journal of Child-Computer Interaction*, 2(2):93-100.

Kim, Y., Kim, I. & Park, N. 2014. Analysis of cyber attacks and security intelligence. Mobile, Ubiquitous, and Intelligent Computing. Springer. p. 489-494).

King, S.T., Tucek, J., Cozzie, A., Grier, C., Jiang, W. & Zhou, Y. 2008. Designing and implementing malicious hardware. *Leet*, 8:1-8.

Kirkpatrick, K. 2017. Financing the dark web. *Communications of the ACM*, 60(3):21-22.

Kirton, H. 2017. Cyber security is too important to be left to the IT department: As hackers increasingly exploit human vulnerability, HR has a vital role to play – not least in ensuring businesses have the technical talent to fight back. *People Management*:42.

Kitzinger, J. 1994. The methodology of focus groups: The importance of interaction between research participants. *Sociology of Health & Illness*, 16(1):103-121.

Kivunja, C. & Kuyini, A.B. 2017. Understanding and applying research paradigms in educational contexts. *International Journal of Higher Education*, 6(5):26-41.

Kjeldskov, J. & Graham, C. 2003. A review of mobile HCI research methods. (In*:* International Conference on Mobile Human-Computer Interaction organised by: Springer. p. 317-335).

Kock, N., Avison, D. & Malaurent, J. 2017. Positivist information systems action research: Methodological issues. *Journal of Management Information Systems*, 34(3):754-767.

Kostewicz, D.E., King, S.A., Datchuk, S.M., Brennan, K.M. & Casey, S.D. 2016. Data collection and measurement assessment in behavioral research: 1958–2013. *Behavior Analysis: Research and Practice*, 16(1):19-33.

Krauss, S.E. 2005. Research paradigms and meaning making: A primer. *Qualitative Report*, 10(4):758-770.

Kritzinger, E. 2017. Growing a cyber-safety culture amongst school learners in South Africa through gaming. *South African Computer Journal,* (2):16.

Krombholz, K., Hobel, H., Huber, M. & Weippl, E. 2015. Advanced social engineering attacks. *Journal of Information Security and Applications*, 22:113-122.

Kshetri, N. 2019. Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2):77-81.

Kuechler, W. & Vaishnavi, V. 2012. A framework for theory development in design science research: Multiple perspectives. *Journal of the Association for Information Systems*, 13(6):395-423.

Kurnava, M. 2016. Cyber-crime v Cyber-attack: What is the difference? https://www.linkedin.com/pulse/cyber-crime-v-cyber-terrorism-what-difference-matthew-kurnava/ Date of access: 29 November 2018.

Lacity, M.C. & Janson, M.A. 1994. Understanding qualitative data: A framework of text analysis methods. *Journal of Management Information Systems*, 11(2):137-155.

Lethbridge, T.C., Sim, S.E. & Singer, J. 2005. Studying software engineers: Data collection techniques for software field studies. *Empirical Software Engineering*, 10(3):311-341.

Lindsay, J.R. 2013. Stuxnet and the limits of cyber warfare. *Security Studies*, 22(3):365-404.

Lombard, E. 2003. Alleged Absa hacker's secrets revealed in court. http://allafrica.com/stories/200309210195.html Date of access: 18 February 2017.

Long, J. 2011. No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing. https://www.hackersforcharity.org/files/NTH_SAMPLE.pdf Date of access: 02 March 2020.

Luo, X., Brody, R., Seazzu, A. & Burd, S. 2011. Social engineering: The neglected human factor for information security management. *Information Resources Management Journal (IRMJ)*, 24(3):1-8.

Mackenzie, N. & Knipe, S. 2006. Research dilemmas: Paradigms, methods and methodology. *Issues in Educational Research*, 16(2):193-205.

Mahlobo, D. 2015. The national cybersecurity policy framework (NCPF) for South Africa. http://cybercrime.org.za/docs/National_Cybersecurity_Policy_Framework_2012.pdf Date of access: 31 May 2019.

March, S.T. & Smith, G.F. 1995. Design and natural science research on information technology. *Decision support systems*, 15(4):251-266.

Masood, R., Um-e-Ghazia, U. & Anwar, Z. 2011. SWAM: Stuxnet worm analysis in Metasploit. (In: Frontiers of Information Technology (FIT) organised by: IEEE p. 142-147).

McCarthy, J. 1980. Circumscription: A form of non-monotonic reasoning. *Artificial Intelligence*, 13(1):27-39.

Mckenney, S. & van den Akker, J. 2005. Computer-based support for curriculum designers: A case of developmental research. *Educational Technology Research and Development,* (2):41.

Mendoza, D.K.O. 2017. The vulnerability of cyberspace-the cyber crime. *Journal of Forensic Sciences & Criminal Investigation*, 2(1):1-8.

Mimecast. 2019. Research finds impersonation, phishing attacks on the rise in South Africa. https://www.defenceweb.co.za/cyber-defence/research-finds-impersonation-phishing-attacks-on-the-rise-in-south-africa/ Date of access: 23 February 2019.

Mitnick, K.D. & Simon, W.L. 2011. *The art of deception: Controlling the human element of security*: John Wiley & Sons.

Morgan, D.L. 1996. FOCUS GROUPS. *Annual Review of Sociology*, 22:129.

Mouton, F., Leenen, L., Malan, M.M. & Venter, H.S. 2014a. Towards an ontological model defining the social engineering domain. *(In* Kimppa, K., Whitehouse, D., Kuusela, T. & Phahlamohlaka, J., *eds*. ICT and Society: 11th IFIP TC 9 International Conference on Human Choice and Computers, HCC11 2014, Turku, Finland, July 30 – August 1, 2014. Proceedings. Berlin, Heidelberg: Springer Berlin Heidelberg. p. 266-279).

Mouton, F., Leenen, L. & Venter, H. 2016. Social engineering attack examples, templates and scenarios. *Computers & Security*, 59:186-209.

Mouton, F., Malan, M.M., Leenen, L. & Venter, H.S. 2014b. Social engineering attack framework. (In*:* Information Security for South Africa (ISSA), 2014 organised by: IEEE. p. 1-9).

Myers, M.D. & Venable, J.R. 2014. A set of ethical principles for design science research in information systems. *Information & Management*, 51(6):801-809.

Ngwenyama, O. 1991. The critical social theory approach to information systems: problems and challenges. p. 267-280).

North-West University. 2010. Rules and guidelines for management of intellectual property at the NWU. Internal document. http://www.nwu.ac.za/sites/www.nwu.ac.za/files/files/i-governance-management/policy/1P-1.1.10_IP_e.pdf Date of access: 2 January 2020.

Oxford English Dictionary. 2001. 3rd ed. Oxford University Press.

Parthy, P.P. & Rajendran, G. 2019. Identification and prevention of social engineering attacks on an enterprise. (In: 2019 International Carnahan Conference on Security Technology (ICCST) organised by: IEEE. p. 1-5).

Passeri, P. 2016. March 2016 cyber attacks statistics. https://www.hackmageddon.com/2016/04/21/march-2016-cyber-attacks-statistics/ Date of access: 18 October 2019.

Patton, S. 2017. The defin-i-tive guide to playtest questions. https://www.schellgames.com/blog/the-definitive-guide-to-playtest-questions Date of access: 28 April 2020.

Peffers, K., Rothenberger, M. & Kuechler, W. 2012. *Design science research in information systems: Advances in theory and practice; 7th international conference, DESRIST 2012, Las Vegas, NV, USA, May 14-15, 2012: proceedings*: Springer.

Peffers, K., Tuunanen, T., Gengler, C.E., Rossi, M., Hui, W., Virtanen, V. & Bragge, J. 2006. The design science research process: A model for producing and presenting information systems research. (In: Proceedings of the first international conference on design science research in information systems and technology (DESRIST 2006) organised by: sn. p. 83-106).

Peffers, K.E.N., Tuunanen, T., Rothenberger, M.A. & Chatterjee, S. 2007. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24(3):45-77.

Petri, G. & von Wangenheim, C.G. 2016. How to evaluate educational games: A systematic literature review. *Journal of Universal Computer Science*, 22(7):992-1021.

Pfleeger, S., Sasse, A. & Furnham, A. 2014. From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, 11(4):489-510.

Pinkas, B. & Sander, T. 2002. Securing passwords against dictionary attacks. (In: Proceedings of the 9th ACM conference on computer and communications security organised by: ACM. p. 161-170).

Plummer-D'Amato, P. 2008. Focus group methodology part 2: Considerations for analysis. *International Journal of Therapy & Rehabilitation*, 15(3):123-129.

Pozo, I.D., Iturralde, M. & Restrepo, F. 2018. Social engineering: Application of psychology to information security. (In: 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) organised by: IEEE. p. 108-114).

Pule, D. 2012. Electronic communications and transactions amendment bill. http://cybercrime.org.za/docs/ECT_Amendment_Bill_2012.pdf Date of access: 29 October 2012.

PWC. 2015. Game of Threats: Responding to cyber threats – how prepared are you? https://www.pwc.co.uk/issues/cyber-security-data-privacy/services/game-of-threats.html Date of access: 06 May 2019.

Rabianski, J.S. 2003. Primary and secondary data: Concepts, concerns, errors, and issues. *Appraisal Journal*, 71(1):43.

Robinson, M., Jones, K. & Janicke, H. 2015. Cyber warfare: Issues and challenges. *Computers & Security*, 49:70-94.

Romand Jr, N.C., Donovan, C., Hsinchun, C. & Nunamaker Jr, J.F. 2003. A methodology for analyzing web-based qualitative data. *Journal of Management Information Systems*, 19(4):213-246.

Sanders, E.B.-N., Brandt, E. & Binder, T. 2010. A framework for organizing the tools and techniques of participatory design. (In: Proceedings of the 11th biennial participatory design conference organised by: ACM. p. 195-198).

Schatz, D., Bashroush, R. & Wall, J. 2017. Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, 12(2):8.

Schilder, J., Brusselaers, M. & Bogaerts, S. 2016. The effectiveness of an intervention to promote awareness and reduce online risk behavior in early adolescence. *Journal of Youth & Adolescence*, 45(2):286-300.

Schlienger, T. & Teufel, S. 2003. Information security culture-from analysis to change. *South African Computer Journal*, 2003(31):46-52.

Scotland, J. 2012. Exploring the philosophical underpinnings of research: Relating ontology and epistemology to the methodology and methods of the scientific, interpretive, and critical research paradigms. *English Language Teaching*, 5(9):9.

Shaw, R.S., Chen, C.C., Harris, A.L. & Huang, H. 2009. The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1):92-100.

Sheng, S., Acquisti, A., Cranor, L., Hong, J., Kumaraguru, P., Mangien, B. & Nunge, E. 2008. Anti-Phishing Phil. http://cups.cs.cmu.edu/antiphishing_phil/ Date of access: 11 February 2020.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J. & 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 3rd symposium on Usable privacy and security organised by: ACM. p. 88-99).

Sim, J. 1998. Collecting and analysing qualitative data: Issues raised by the focus group. *Journal of Advanced Nursing*, 28(2):345-352.

Simon, H.A. 1996. *The sciences of the artificial*. 3rd ed: MIT press.

Singer, P.W. 2015. Stuxnet and its hidden lessons on the ethics of cyberweapons. *Case Western Reserve Journal of International Law*, 47(3):79-86.

Singh, A. & Singh, A. 2017. Review of cyber threats in social networking websites. *International Journal of Advanced Research in Computer Science*, 8(5):2695-2699.

Slevitch, L. 2011. Qualitative and quantitative methodologies compared: Ontological and epistemological perspectives. *Journal of Quality Assurance in Hospitality & Tourism*, 12(1):73-81.

Sood, A.K. & Enbody, R.J. 2014. *Targeted cyber attacks: Multi-staged attacks driven by exploits and malware*: Amsterdam; Boston: Syngress, 2014.

Spinuzzi, C. 2005. The methodology of participatory design. *Technical Communication*, 52(2):163-174.

Stiawan, D., Idris, M.Y., Abdullah, A.H., Aljaber, F. & Budiarto, R. 2017. Cyber-attack penetration test and vulnerability analysis. *International Journal of Online Engineering*, 13(1):125-132.

Takeda, H., Veerkamp, P. & Yoshikawa, H. 1990. Modeling design process. *AI Magazine*, 11(4):37-48.

The joint chiefs of staff. 2011. Memorandum for chiefs of the military services. http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf Date of access: 29 November 2018.

Thomson, S. 2011. Qualitative research: Validity. *Joaag*, 6(1):77-82.

Trauth, E. & Jessup, L. 2000. Understanding computer-mediated discussions: Positivist and interpretive analyses of group support system use. *MIS Quarterly*, 24(1):43-79.

Unity. 2020. Asset Store Terms of Service and EULA. https://unity3d.com/legal/as_terms?_ga=2.27843519.283365715.1587459950-814353672.1584085890 Date of access: 21 April 2020.

Vaishnavi, V., Kuechler, W., Petter, S. & De Leoz, G. 2004/2019. Design science research in information systems. http://desrist.org/design-research-in-information-systems/ Date of access: 18 April 2020.

Van den Akker, J., Branch, R.M., Gustafson, K., Nieveen, N. & Plomp, T. 2012. *Design approaches and tools in education and training*: Springer Science & Business Media.

van Heerden, R., Irwin, B., Burke, I.D. & Leenen, L. 2012. A computer network attack taxonomy and ontology. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 2(3):12-25.

van Heerden, R., von Solms, S. & Vorster, J. 2018. Major security incidents since 2014: An African perspective. (In: 2018 IST-Africa Week Conference (IST-Africa) organised by: IEEE. p. 1-11).

van Heerden, R., von Soms, S. & Mooi, R. 2016. *Classification of cyber attacks in South Africa*. Paper presented at the IST-Africa Week Conference, Durban, South Africa, 11 May 2016. https://nwulib.nwu.ac.za/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edseee&AN=edseee.7530663&site=eds-live Date of access: 16 April 2020.

van Niekerk, B. 2017. An analysis of cyber-incidents in South Africa. *African Journal of Information and Communication*, 20:113-132.

von Solms, B. & von Solms, R. 2018. Cybersecurity and information security: what goes where? *Information & Computer Security*, 26(1):2-9.

von Solms, R. & van Niekerk, J. 2013. From information security to cyber security. *Computers & Security*, 38:97-102.

Walliman, N. 2011. *Research methods: The basics*. London: Routledge.

Wang, X., Kohno, T. & Blakley, B. 2014. Polymorphism as a defense for automated attack of websites. (In: International Conference on Applied Cryptography and Network Security organised by: Springer. p. 513-530).

Warwick, A. 2016. Social engineering confirmed as top information security threat. http://www.computerweekly.com/news/4500273577/Social-engineering-confirmed-as-top-information-security-threat Date of access: 19 February 2017.

Wenjun, F., Lwakatare, K. & Rong, R. 2017. Social engineering: I-E based model of human weakness for attack and defense investigations. *International Journal of Computer Network & Information Security*, 9(1):1-11.

Whitson, G. 2019. Cybercrime. In: *Salem Press Encyclopedia*: https://nwulib.nwu.ac.za/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=ers&AN=89138922&site=eds-live Date of access: 18 April 2020.

Williams, C. 2007. Research methods. *Journal of Business & Economic Research*, 5(3):65-72.

Winkler, I.S. & Dealy, B. 1995. *Information security technology? Don't rely on it: A case study in social engineering*. Paper presented at the USENIX Security Symposium. https://www.usenix.org/publications/library/proceedings/security95/full_papers/winkler.pdf Date of access: 16 June 2020.

Wolf, M.J. & Fresco, N. 2016. Ethics of the software vulnerabilities and exploits market. *Information Society*, 32(4):269-279.

Xiangyu, L., Qiuyang, L. & Chandel, S. 2017. Social engineering and insider threats. (In*:* 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) organised by: IEEE. p. 25-34).

Zhang, C. & Xiao, J. 2018. Stability analysis of an advanced persistent distributed denial-of-service attack dynamical model. *Security & Communication Networks*:1-10.

APPENDIX A: RESEARCHER'S CODE OF CONDUCT

NORTH-WEST UNIVERSITY
YUNIBESITI YA BOKONE-BOPHIRIMA
NOORDWES-UNIVERSITEIT

Research and Innovation

CODE OF CONDUCT FOR RESEARCHERS

This code of conduct is applicable to all NWU researchers.

As a researcher of the North-West University (NWU), I subscribe to the rules of the NWU Senate Committee for Research Ethics (SCRE), all applicable policies of the NWU as well as all national and international laws and regulations applicable to my field of study. Furthermore, I commit myself to abide by the ethical principles and responsibilities as set out in the Singapore statement on Research Integrity (22 September 2010), in any and all research endeavours that I undertake as a researcher of the NWU.

The four major principles of research integrity to which I will adhere and that will guide my research are:

- Honesty in all aspects of research;
- Accountability in the conduct of research;
- Professional courtesy and fairness in working with others;
- Good stewardship of research on behalf of others.

Consequently I will also adhere to the following ethical responsibilities:

1. I will take responsibility for the originality and trustworthiness of my research.

2. I will stay abreast of and adhere to all institutional, national, and international laws, regulations, and policies applicable and related to my research.

3. I will at all times employ appropriate research methods, base my conclusions on critical analysis of the evidence and report my findings and interpretations fully and objectively.

4. I will keep clear and accurate records of all research that I have conducted in a manner that will allow verification and replication of my work by others, if applicable.

5. I will, where applicable, share my data and findings openly and promptly, in line with external funding rules. This will be done as soon as possible after I have had an opportunity to establish priority and ownership claims.

6. I will take responsibility for my own contributions to publications, funding applications, reports and other representations of my research. I will also and only include authors who meet valid authorship criteria.

7. I will acknowledge the names and roles of those who made significant contributions to my research in publications, including writers, funders, sponsors, and others, but do not meet authorship criteria.

8. In my peer reviews, I will provide fair, prompt and rigorous evaluations and I will respect confidentiality when I review others' work.

9. I will disclose all conflicts of interest (financial and other) that could compromise the trustworthiness of my work in research proposals, publications, public communications, and in review activities.

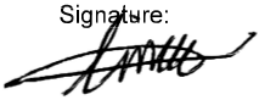
10. When I publically address a community in the spirit of academic freedom, I will in all stages base my professional comments on research findings (if applicable) and my expertise. I will distinguish between professional comments and opinions based on personal views.

11. Should any irresponsible research practices and/or research misconduct become known to me or brought under my attention, I will report such irresponsible research activities to the appropriate authorities.

12. I will respond to irresponsible research practices or conduct, by taking prompt actions as set out in the procedures of the university. I will also protect those who report misconduct in good faith, to the best of my abilities.

13. I will endeavour to create and sustain an environment that encourage research integrity through education of students, research teams and peers, as well as abide by policies, and reasonable standards for advancement.

14. I will at all times weigh societal benefits against the risks inherent in my work.

Name:	Signature:	Date:
Ian Loyiso Ngqoyiyana		May 2017

Original details: (11664754) P:\9. Research and Post-graduate Education\9.1 Implementation of the research strategy\9.1.5 Ethics\9.1.5.1.3_Code_Conduct_2017.docm
18 July 2017

File reference: 9.1.5.1.3

APPENDIX B: ETHICAL CLEARANCE

Faculty of Natural and Agricultural Sciences
Ethics Committee
Private Bag x6001, Potchefstroom,
2520, South Africa
Web: http://www.nwu.ac.za

Tel: +27-18-299-2521
Fax: +27-18-299-2503
Email: oriel.thekisoe@nwu.ac.za
Date: 04 Sep 2019

To: Mr Ngqoyiyana

RE: Approval of your application by the FNAS Ethics Committee

Ethics number: NWU-01177-19-S9

Study title: Developing an artefact for raising social engineering awareness among administrative staff

Study leader: JT Janse van Rensburg

Student: Mr IL Ngqoyiyana

You are kindly informed that after review by the FNAS Ethics committee, North-West University, your ethics approval application has been successful.

Your study has been approved as a **Low Risk** project with the following conditions.

- Informed consent must be submitted to committee in case of questionnaire survey.
- Permission letter from study area owner/authority e.g. farmer, manager etc.
- You must submit monitoring report/progress report of study mid-year to commencement of study and after completion of the study.

Yours sincerely,

Prof. Oriel Thekisoe

Acting Chairperson

FNAS Ethics Committee

APPENDIX C: CONSENT FORM TEMPLATE – NWU

Private Bag X1290, Potchefstroom
South Africa 2520
Tel: +2718 299-1111/2222
Fax: +2718 299-4910
Web: http://www.nwu.ac.za

The Faculty of Natural and Agricultural Sciences Ethics Office of the North-West University is acknowledged for the use of their document with minor adjustments made by the North-West University Education, Management and Economic Sciences, Law, Theology, Engineering and Natural Sciences Research Ethics Committee (NWU-EMELTEN-REC).

NWU-EMELTEN-REC Stamp

INFORMED CONSENT DOCUMENTATION FOR HOSTING A WORKSHOP WITH ADMINISTRATIVE STAFF

TITLE OF THE RESEARCH STUDY: Exploring cyber security: A DSR approach

ETHICS REFERENCE NUMBERS: NWU-001177-19-S9

PRINCIPAL INVESTIGATOR: Mrs. JT Janse van Rensburg

POST GRADUATE STUDENT: Ian Loyiso Ngqoyiyana

ADDRESS:
23 Lethabo Street,
Vaalpark,
1947

CONTACT NUMBER: +27(0) 78 084 2430 | +27(0) 11 304 5211

You are being invited to take part in a **research study** that forms part of a Masters study. Please take some time to read the information presented here, which will explain the details of this study. Please ask the researcher, or person explaining the research to you, any questions about any part of this study that you do not fully understand. It is very important that you are fully satisfied that you clearly understand what this research is about and how you might be involved. Also, your participation is **entirely voluntary** and you are free to say no to participate. If you say no, this will not affect you negatively in any way whatsoever. You are also free to withdraw from the study at any point, even if you do agree to take part now.

This study has been approved by the **North-West University Natural and Agricultural Sciences Research Ethics Committee (NWU*)** and will be conducted according to the ethical guidelines and principles of Ethics in Health Research: Principles, Processes and Structures (DoH, 2015) and other international ethical guidelines applicable to this study. It might be necessary for the research ethics committee members or other relevant people to inspect the research records.

What is this research study all about?

- *We plan to design a serious game that can be used to raise awareness around social engineering attacks.*
- *This study will be conducted at the NWU Vaal Triangle campus and other medium to large size organisation. The study will be done by experienced computer science researchers trained in the field of design science research.*
- *Approximately four participants will be included in the initial design of this study.*
- *Additional participants may be included in the study as necessary for data gathering and evaluation purposes.*

Why have you been invited to participate?

- *You have been invited to be part of this research because you meet the specific criteria that is required to satisfy one of the design areas in this study.*
- *You have also been selected because your exposure to the area of this design is also relevant.*
- *You will unfortunately not be able to take part in this research if you specifically do not agree with this consent form or are not comfortable with participating in the topic of this study.*

What will be expected of you?

- *You will be expected to attend a brief workshop that will require you answer a questionnaire and to interact with an artefact.*

Will you gain anything from taking part in this research?

- *The gains for you if you take part in this study will be that you may learn new concepts regarding cyber security and social engineering.*
- *You may also learn how to prevent yourself from being a victim of social engineering attacks.*
- *The other indirect gains of the study is in that you will be contributing to the design of an artefact that could build on knowledge for solving a problem that is faced by people on a pandemic scale.*

Are there risks involved in you taking part in this research and what will be done to prevent them?

- *The risks to you in this study are that you may develop a small fear for trusting computing devices in your daily usage, but this risk will be limited by providing you with an explanation during the workshop as to why you shouldn't worry.*
- *There are more gains for you in joining this study than there are risks.*

How will we protect your confidentiality and who will see your findings?

- *Anonymity of our findings will be protected by removing all personally identifiable information. Your privacy will be respected by ensuring that the information collected will only be information that is directly relevant to the study and does not infringe on your personal privacy in any form. Your results will be kept confidential and will only be accessible by the researchers directly involved in this study. Only the researchers and relevant faculty heads will be able to look at our findings. Findings will be kept safe by locking hard copies in secured storages and for electronic data, it will be password protected. As soon as data has been transcribed it will be deleted from the recorders. Data will be stored for approximately 6 months from date of completion of the research.*

What will happen with the findings or samples?

- *The findings of this study will only be used for this study but may be referenced directly from this study in future research. No personally identifiable information will be included in any of the findings.*

How will you know about the results of this research?

- We will give you the results of this research when the research is complete or if you directly request for them during the study.
- You will be informed of any new relevant findings by directly emailing the researcher.

Will you be paid to take part in this study and are there any costs for you?

- This study is not directly funded by any entity, it is self-funded by the researcher.
- **Please note:** you will not be paid to take part in the study because this research does not have any direct fund for participation.
- No travel expenses will be paid to participants.
- Refreshments will be served during the workshop.
- There will be no costs involved for you, if you do take part in this study.

Is there anything else that you should know or do?

- You can contact JT Janse van Rensburg (+27 82 582 4352), Japie Greeff (+27 72 403 1221) or Ian Ngqoyiyana (+27 78 084 2430) if you have any further questions or have any concerns.
- You can also contact the North-West University Natural and Agricultural Sciences Research Ethics Committee via Mrs Marlize Bisschoff at 018 299 4707 or marlize.bisschoff@nwu.ac.za if you have any concerns that were not answered about the research or if you have complaints about the research.
- You will receive a copy of this information and consent form for your own purposes.

Declaration by participant

By signing below, I ……..……. agree to take part in the research study titled: Exploring cyber security: A DSR approach

I declare that:

- I have read this information/it was explained to me by a trusted person in a language with which I am fluent and comfortable.
- The research was clearly explained to me.
- I have had a chance to ask questions to both the person getting the consent from me, as well as the researcher and all my questions have been answered.
- I understand that taking part in this study is **voluntary** and I have not been pressurised to take part.
- I may choose to leave the study at any time and will not be handled in a negative way if I do so.
- I may be asked to leave the study before it has finished, if the researcher feels it is in the best interest, or if I do not follow the study plan, as agreed to.

Signed at (*place*) .....…..…….. on (*date*) ……...…….. 20....

....
Signature of participant **Signature of witness**

Declaration by person obtaining consent

I *(name)* ……..…… declare that:

- I clearly and in detail explained the information in this document to:

  (participant)…….
- I did/did not use an interpreter.
- I encouraged him/her to ask questions and took adequate time to answer them.
- I am satisfied that he/she adequately understands all aspects of the research, as discussed above
- I gave him/her time to discuss it with others if he/she wished to do so.

Signed at (*place*) .....…..…….. on (*date*) ……...…….. 20....

.....
Signature of person obtaining consent

Declaration by researcher

I *(name)* ……..…… declare that:

- I explained the information in this document to …….. .
- I did/did not use an interpreter
- I encouraged him/her to ask questions and took adequate time to answer them.
- The informed consent was obtained by an independent person.
- I am satisfied that he/she adequately understands all aspects of the research, as described above.
- I am satisfied that he/she had time to discuss it with others if he/she wished to do so.

Signed at (*place*) .....…..……. on (*date*) ……...…….. 20....

.....
Signature of researcher

APPENDIX D: PARTICIPATORY DESIGN: PARTICIPANT DETAILS

In a participatory design strategy, different role players provide insight and guidance into the research process. These will include participants from the target user group who provided feedback on developed artefacts, as well as various experts who may provide insight into critical knowledge areas of the research.

In this appendix, an overview is provided of all role players who formed part of the participatory design strategy in this study. Expert participants are coded using E as a reference, and participants who form part of the target user group for designing and developing the artefact are referenced with P. The participants involved in the ***reaction*** level evaluation of the artefact are referenced with RP. The participants involved in the ***learning*** level evaluation of the artefact are referenced with LP.

Details for participants who formed part of the participatory design process for the research process and research methodology (Chapter 1 and Chapter 2), included:

Expert #	Type/role	Contribution	Experience
E1	Design science research expert (academic)	Reviewed the literature content and guided the study	7 years DSR expert
E2	Design science research expert (academic)	Reviewed the literature content and guided the study	8 years DSR expert

Details for participants who formed part of the participatory design process for literature review content (Chapter 3), included:

Expert #	Type/role	Contribution	Experience
E1	Design science research expert (academic)	Reviewed the literature content and guided the study	7 years DSR expert
E2	Design science research expert (academic)	Reviewed the literature content and guided the study	8 years DSR expert
E3	Cyber-security expert (industry)	Reviewed literature content on cyber-security and social engineering and made suggestions towards improvement	4 years software developer and 3 years penetration tester

Details for participants who formed part of the participatory design process for the development methodology (Chapter 4), included:

Expert #	Type/role	Contribution	Experience
E1	Design science research expert (academic)	Reviewed the literature content and guided the study	7 years DSR expert
E2	Design science research expert (academic)	Reviewed the literature content and guided the study	8 years DSR expert

Details for participants who formed part of the participatory design process (as workshop 1 and 2) for pre-artefact development (Chapter 5), included:

Expert & participant #	Type/role	Contribution	Experience
E1	Design science research expert (academic)	Reviewed the mood board design and its write-up and made further recommendations for improvement	7 years DSR expert
E2	Design science research expert (academic)	Reviewed the mood board design and suggested improvements	8 years DSR expert
E4	Design artist	Made recommendations on the design considerations of a mood board and suggested improvements	9 years freelance graphic designer
Target user group participants from Company A			
P1	Administrator	Provided input into the requirements gathering phase for the conceptual design and concept validation at the end of the conceptual design	14 years administrative staff
P2	Administrator	Provided input into the requirements gathering phase for the conceptual design concept validation at the end of the conceptual design	24 years administrative staff
P3	Administrator	Provided input into the requirements gathering phase for the conceptual design concept validation at the end of the conceptual design	10 years secretary staff, more than 1 year finance staff
P4	Administrator	Provided input into the requirements gathering phase for the conceptual design concept validation at the end of the conceptual design	21 years administrative staff

Details for participants who formed part of the participatory design process (as workshop 3) for mid-artefact development (Chapter 6), included:

Expert & participant #	Type/role	Contribution	Experience
E1	Design science research expert (academic)	Reviewed the mood board design and its write-up and made further recommendations for improvement	7 years DSR expert

E2	Design science research expert (academic)	Reviewed the mood board design and suggested improvements	8 years DSR expert
Target user group participants from Company B			
P5	Administrator	Provided input into the improvement of the presented prototype 1	4 years administrative staff (secretary)
P6	Administrator	Provided input into the improvement of the presented prototype 1	7 years administrative staff (receptionist)
P7	Cyber-security professional	Provided input into the improvement of the presented prototype 1	4 years cyber-security
P8	Cyber-security professional	Provided input into the improvement of the presented prototype 1	7 years business continuity and crisis management 2 years cyber-security

Details for participants who formed part of the participatory design process for post-artefact development (Chapter 7), included:

Expert #	**Type/role**	**Contribution**	**Experience**
E1	Design science research expert (academic)	Reviewed the prototype 1 write-up and made suggestion for improvement	7 years DSR expert
E2	Design science research expert (academic)	Reviewed the prototype 1 design and made design recommendations for improvement	8 years DSR expert

Details for participants who formed part of the participatory design process for reporting on the ***reaction*** level evaluation of the artefact in Section 7.3.1 (Chapter 7), included:

Expert #	**Feedback role**	**Contribution**	**Experience**
E1	Design science research expert (academic)	Guided the design of the reaction evaluation process	7 years DSR expert
E2	Design science research expert (academic)	Provided evaluation guidance input where applicable	8 years DSR expert

Target user group participants from both Company A and Company B			
Reaction participant #	Feedback role	Sector	Experience

RP1	Administrative/support role	Academic sector	6 years
RP2	Design expert	Academic sector	9 years
RP3	Design expert	Academic sector	4 years
RP4	Cyber security professional	Industry sector	4 years

Details for participants who formed part of the participatory design process for reporting on the ***learning*** level evaluation of the artefact in Section 7.3.2 (Chapter 7), included:

Expert #	**Feedback role**	**Contribution**	**Experience**
E1	Design science research expert (academic)	Guided the design of the learning evaluation process	7 years DSR expert
E2	Design science research expert (academic)	Provided evaluation guidance input where applicable	8 years DSR expert

Target user group participants from Company B			
Learning Participant#	**Feedback role**	**Contribution**	**Experience**
LP1	Administrator	Completed the pre- and post-test questionnaire for testing the game-based artefact	11 years 4 months, senior secretary
LP2			12 years 1 month, business operations senior consultant
LP3			7 years 4 months, finance administrator
LP4			6 months, senior clerk
LP5			6 years 2 months, senior administrator
LP6			4 months, project services accountant
LP7			9 years 10 months, senior secretary
LP8			5 years, strategic and reputational risk consultant
LP9			5 years 11 months, senior administrator
LP10			13 years 8 months, senior administrator
LP11			10 months, junior internal accounting

			project services administrator
LP12			20 years 2 months, executive secretary
LP13			11 years 2 months, business reputational risk learning experience manager
LP14			14 years 10 months, junior administrator
LP15			5 years 5 months, strategic and reputational risk senior consultant

The total number of experts and participants who were involved in this study are 27 unique individuals and are categorised as follows:

- Four (4) experts – two of whom were design experts, one cyber-security expert, and one expert design artist;
- Four (4) participants from organisation A – the four participants are administrators who were from organisation A and participated in the design and development of the conceptual prototype in workshops 1 and 2;
- Four (4) participants from organisation B – the four participants from organisation B are a mix of cyber-security professionals and administrators from organisation B who participated in the design and development of the final prototype as workshop 3; and
- Fifteen (15) participants from organisation B – the 15 participants from organisation B are mainly secretaries, general business administrators, finance and accounts administrators, as well as internal business reputational risk administrators.

APPENDIX E: OPEN-CODED RESULTS FROM WORKSHOP 1

The table below provides a coded summary of the key themes noted during workshop 1 where design requirements were gathered from target user group participants.

Coded summary of the key themes noted in the first requirements gathering workshop

Code	Description within context of workshop feedback
Theme 1: Platform	
Computer-/laptop-based game (1 occurrence)	The game could be played on a desktop computer or laptop
Mobile device-based game (1 occurrence)	The game could be played on a mobile device
Any device platform (1 occurrence)	Any platform for designing the game is fine
Theme 2: Character	
Character/avatar could be customisable (2 occurrences)	The characters the users will be using could be selectable or customisable (either based on role or custom design, i.e. skin colour, hat colour, etc.)
Character/avatar could look like a real-world character (1 occurrence)	The different characters/avatars the user will interact with could look like they would in the real wold (i.e. the characters could be relatable in the real-world)
Theme 3: Mechanics	
In-game time limit (6 occurrences)	The game could have a time limit (+- 1 minute) for a player to complete each challenge
Yes/No questions to be answered for points (1 occurrence)	The game should not be multi-choice, but could use Yes/No answers to questions
Multi-player capability (2 occurrences)	The game could allow multiple players to challenge one another, either through scores or inter-gameplay
Multi-level game capability (3 occurrences)	The game could be able to move between multiple levels
Points/scoring system (6 occurrences)	The game could keep the player's score/points throughout the game
Player scoreboard history (2 occurrences)	The game could save the player's scoreboard, and maybe also track other users' scores on one board

Code	Description within context of workshop feedback
Save game progress to continue later (4 occurrences)	The game could allow the player to save the game and continue at a later time where they left off
End of game feedback/report (1 occurrence)	The game could provide a player with a report at the end of the gaming showing a summary of the player's entire game play results (time, points, etc.)
Closed levels that prevent user from proceeding without passing challenge (1 occurrence)	The game could be closed and not enable the player to proceed to next level until they win the current level
In-game video narrations to explain concepts (2 occurrences)	The game could have video-based narrations to explain key concepts
Multiple scenarios explaining the concepts for each level (2 occurrences)	The game could allow multiple scenarios to be generated for a level that explains a specific concept (i.e. many scenarios for one concept in a level)
In-game instructions (1 occurrence)	The game could provide the player with instructions on what to do during the game
Theme 4: UI Design	
Heads up display to display game progress (4 occurrences)	Display player's current progress to show when the game will be completed – player could be able to track where they are
Design could relate to target users (6 occurrences)	The design of the game could relate to the specific organisation type (e.g. academic, legal, consulting, etc.)
Scenarios could be real-world scenarios (4 occurrences)	The scenarios could relate to real-world scenarios that the target users would typically be confronted with
Game design could be easy to understand ("no brainer") (4 occurrences)	The game could not require too much thinking, it could be more entertaining/fun
Game design could be challenging (3 occurrences)	The game could be challenging and require a user to think
Game design could not be a 2-D based game (2 occurrences)	The game should not be comical in its design, as it is an artefact about a serious topic and could therefore not look cartoonish
Any camera mode can be used to represent game (1 occurrence)	No specific camera mode

APPENDIX F: FIRST AND SECOND MOOD BOARD EVALUATION

The evaluation of the first mood board was performed by the design science research experts and a design artist. They examined the first mood board and indicated that the design was not adequate. They provided recommendations regarding corrective actions such as the following:

- The in-game questions design should logically allow for an in-game scoreboard;
- The colour pallet should align to the theme in the mood board;
- Emphasis should be placed on keywords such as social engineering;
- The images used in the design should as close as possible represent the intended design;
- The images that overlap with each other should be of related concepts; and
- The selected icons and images should clearly specify the intended concepts.

The design artist recommended that general mood boards could be used for guidance to develop a mood board (such as the example mood boards provided below). The theme that is clear from the design artist's recommendations is that the mood board should clearly reflect the key concepts for the design and depict related images.

Mood board example 1

Mood board example 2

APPENDIX G: OPEN-CODED RESULTS FROM WORKSHOP 2

During the second workshop that was held pre-artefact, participants from the target user group were presented with the conceptual mood board and conceptual prototype.

A series of questions were asked that touched on the criteria defined by Mckenney and van den Akker (2005:48). Some of the questions presented to the participants included:

- Are the elements presented in the conceptual design in line with the elements identified in the prior workshop?
- Are there specific design elements that were presented that you would like changed?
- Is the platform presented still suitable to your needs?
- Do you think this tool would better equip you to become more aware of social engineering attacks? and
- Anything in particular you would like to change?

The table below provides a coded summary of the key themes noted during workshop 2 feedback where confirmation of design requirements captured during workshop 1 was discussed.

Code	Description within context of workshop feedback
Theme 1: Platform	
Computer/laptop based game (4 occurrences)	The game should be played on a desktop computer or laptop
Theme 2: Character	
N/A	N/A
Theme 3: Mechanics	
Challenging game (3 occurrences)	The game should not have simple Yes/No questions, but should engage the player to apply their mind more.
Capturing user information (2 occurrences)	The game should track the user information before playing the game; this information should be reflected during game play to make the game more personal to the player.
In-game instructions/help (2 occurrences)	The game should constantly provide the player with instructions or a help function to guide them if they have any progression challenges.
Videos to explain concepts (1 occurrence)	The game should have videos that explain difficult concepts to the player.

Code	Description within context of workshop feedback
Theme 4: UI Design	
Lighter game theme (4 occurrences)	The game should have a brighter theme. A darker theme makes the game unappealing to the player.
Better readable font (3 occurrences)	The game font should be larger and clearly readable to the player.

From the themes identified in the table above, it is clear that the participants preferred a desktop-based artefact over other platforms. This is because the participants felt more comfortable in playing a game-based artefact on their workstation. Another reason was that they spend extended time on the desktop-based platform performing their daily work activities.

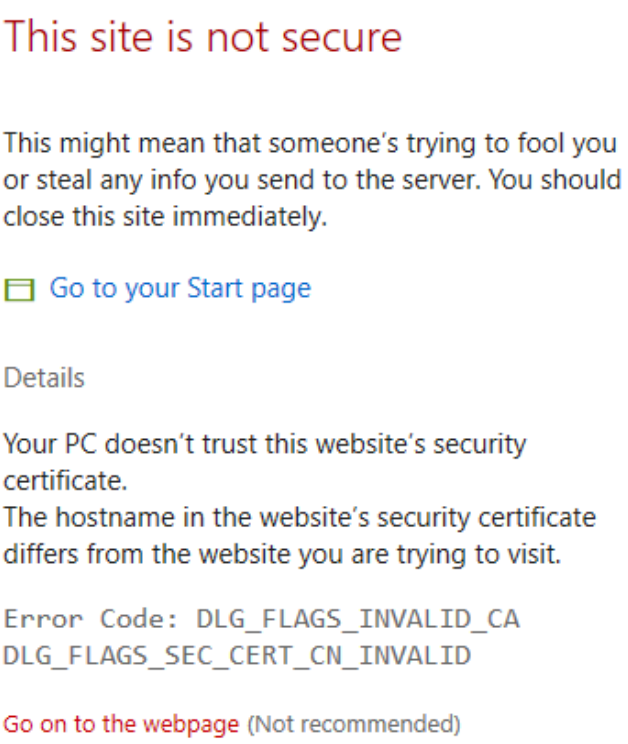
APPENDIX H: PROTOTYPE 1 REVISION (REVISION 1 – EXPERT FEEDBACK)

An open-ended test of the artefact is performed by the design experts in the development of the working prototype. It is important to note that the design of this prototype is an extension of the conceptual design (as discussed in Chapter 5). The responses from the design experts for the design interfaces are depicted below.

(a) Unsafe landing page

The landing page of the game did not have a valid certificate and therefore provided the user with the error depicted in below.

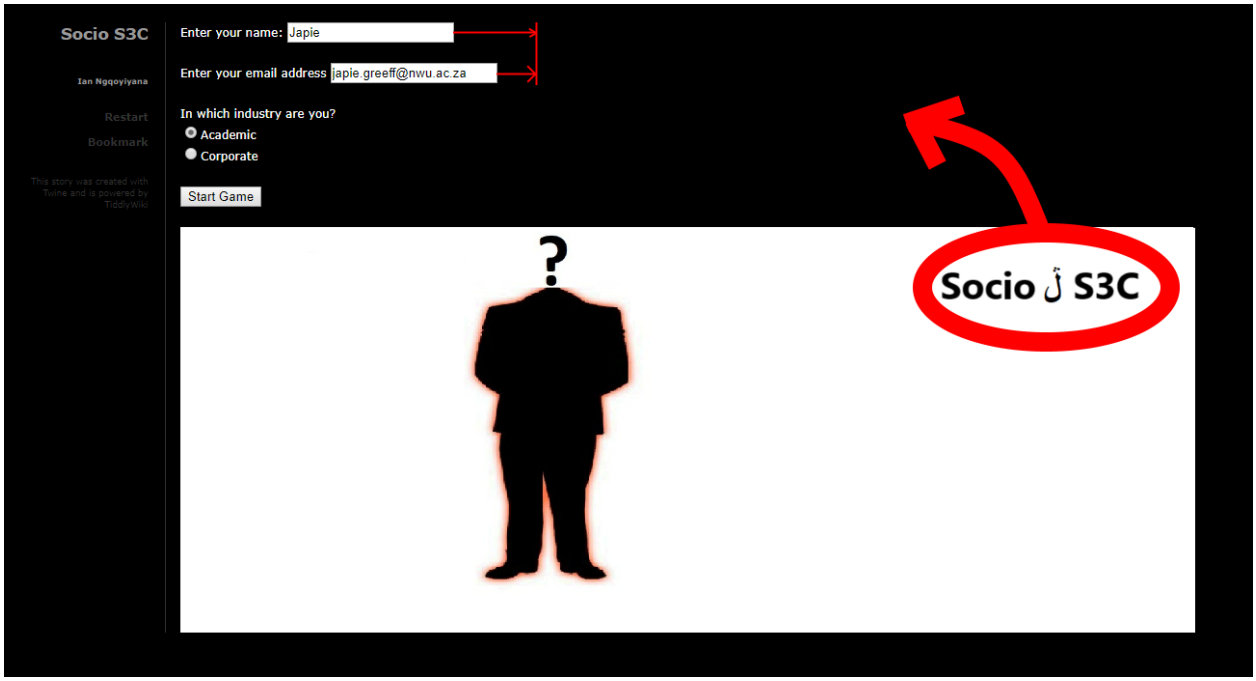
The game-landing page used an invalid certificate



(b) Start screen

The screen is very dark. The name of the game should be placed on the large black space on the top right part of the screen. The two text boxes to the right should have been aligned.

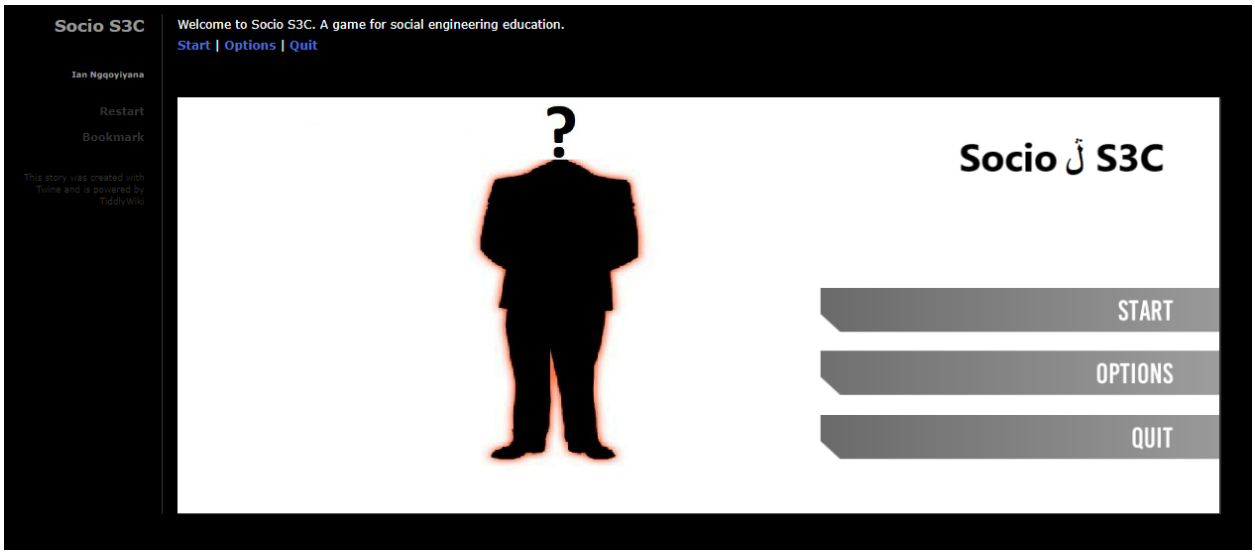
Design issues with the game start screen



(c) Start Screen 2

The buttons on the start screen image should have been made clickable. Image map is used to achieve this design requirement.

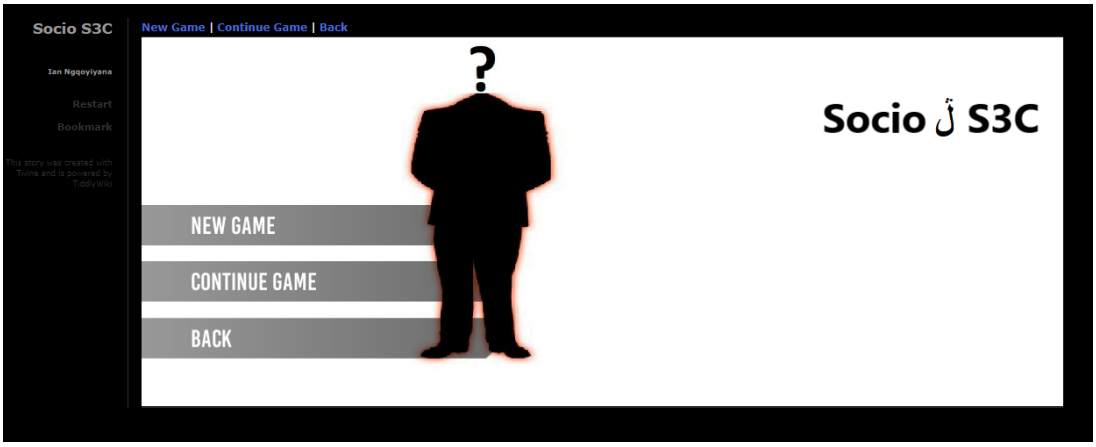
Start screen buttons should be made clickable



(d) Start screen 3

The button styles are inconsistent to those of the previous screen's (start screen) buttons.

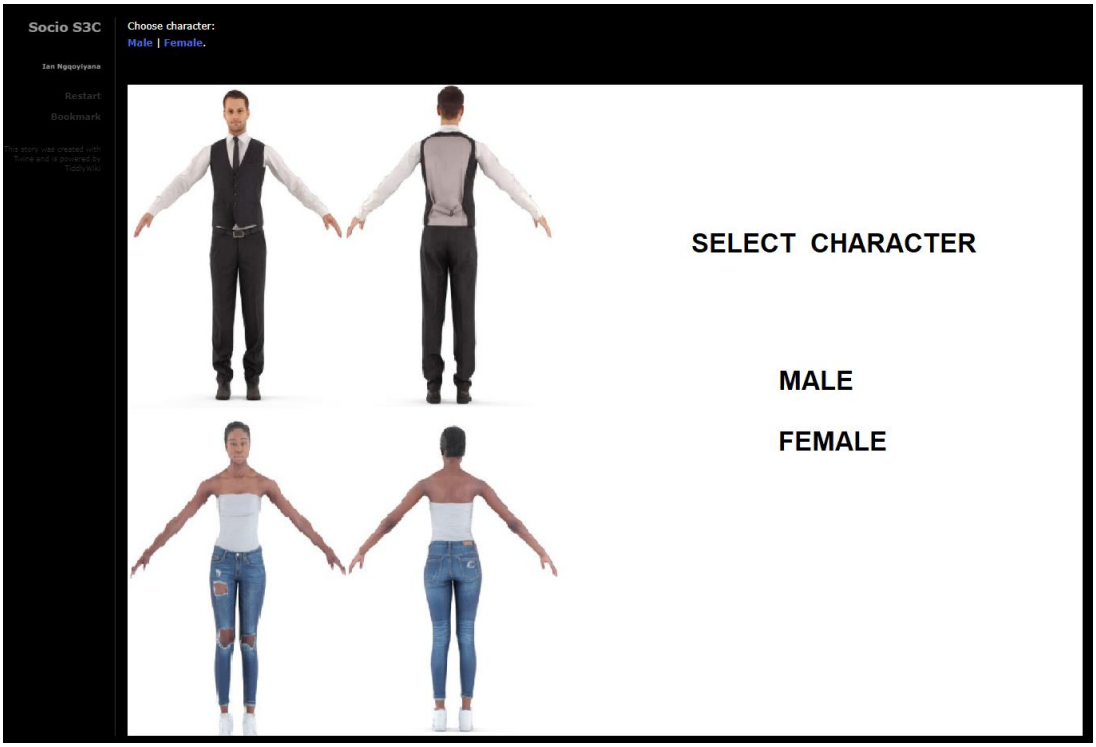
Inconsistent button styles between screens



(e) Character select screen

The characters did not show consistent design, specifically around the dress code.

Inconsistent character theme



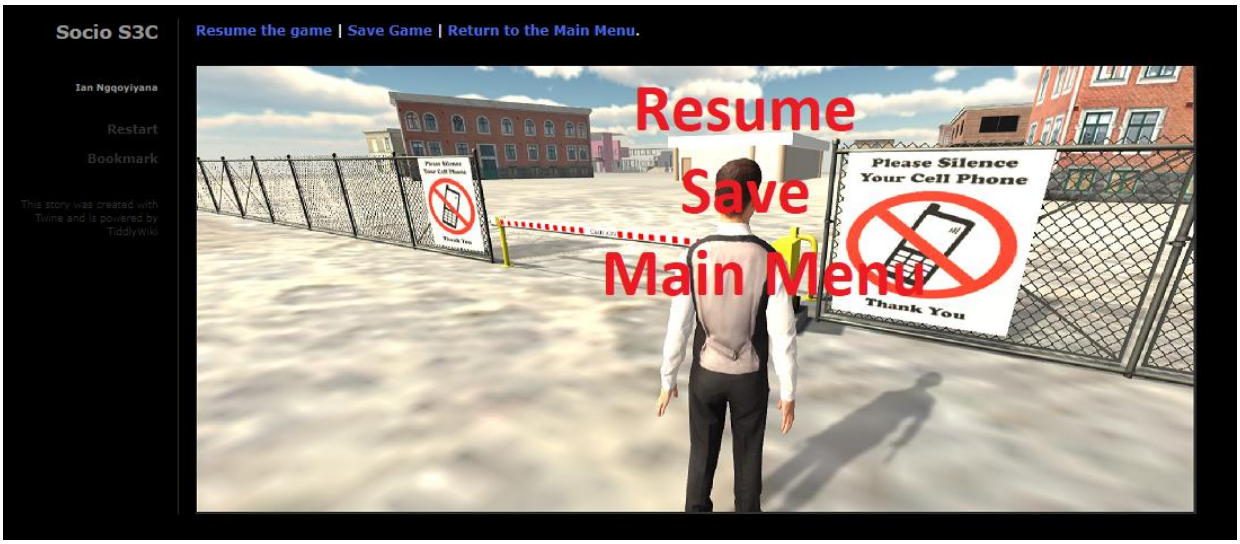
(f) Intro Screen

The character selection button did not change the character when playing the actual game.

Malfunctioning character select option

Text in the game switches between lowercase and uppercase. The game menu text styling is not consistent with that of the game start menus.

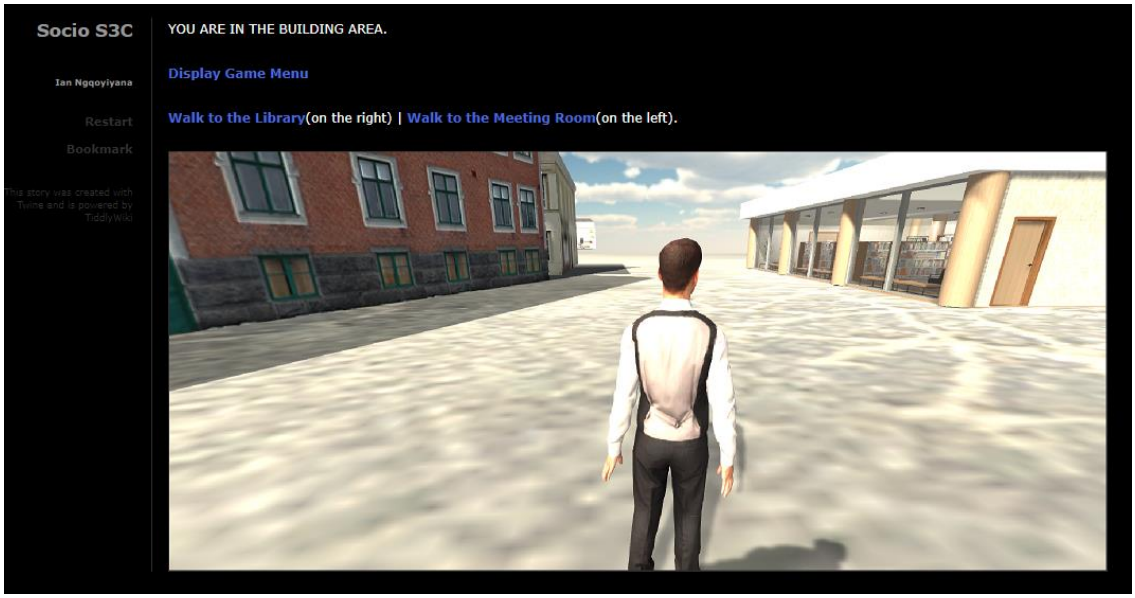
Inconsistent text casing and menu text styling



(g) Facility screen

The action buttons are not on the correct side, i.e. the left-hand option is the library (on the right), and the right-hand option is the meeting room (on the left), when it should be the other way around.

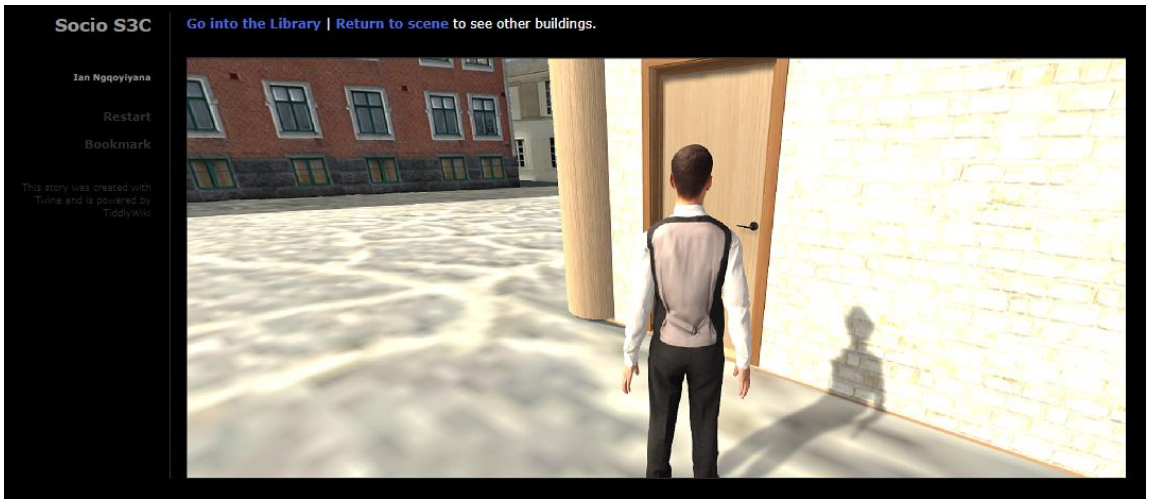
Action buttons on the incorrect sides



Library scene 1

There is no menu screen. The player has no context where they are. The library entrance should have been more ornate.

Design shortfalls at the library entrance scene



(h) Read email on computer

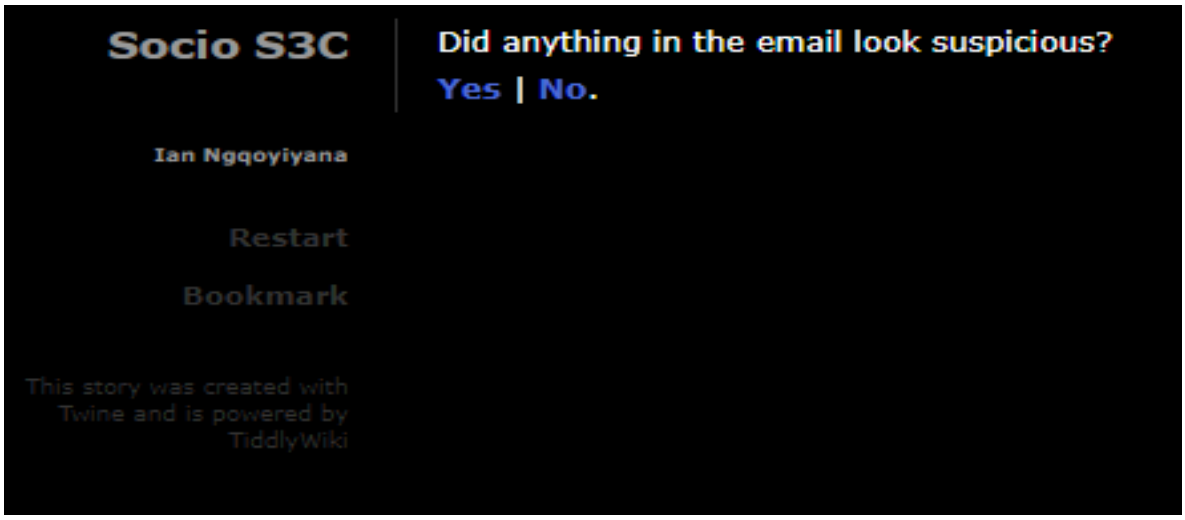
The email reader screen served no purpose, and should rather allow a user to go straight into the email, or alternatively have a couple of emails that can be clicked.

Screen that serves no purpose

(i) Read email on computer continued

No autonomy is available at this point. The game should present more than just yes/no questions.

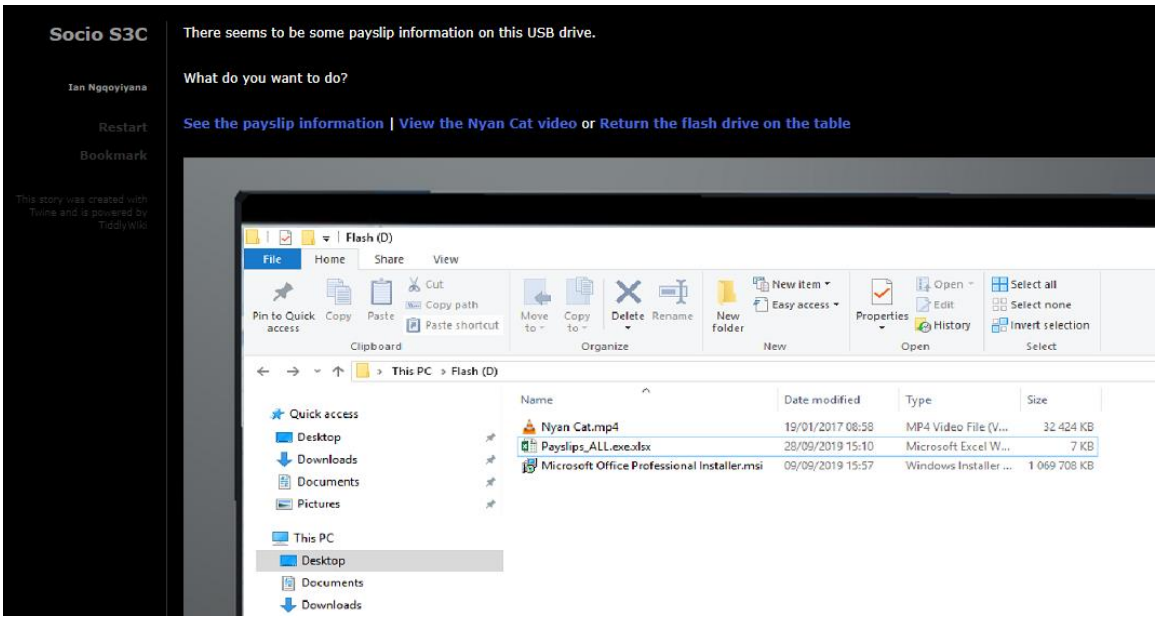
No autonomy in yes/no questions



(j) Plug in the flash drive

There should be more interactive functionality for the screen and should allow a user to click and visually experience the interaction.

Limited interactive functionality



The section that follows shows the results from the second revision by the design experts after the recommendations described above are corrected/implemented.

APPENDIX I: PROTOTYPE 1 REVISION (REVISION 2 – EXPERT FEEDBACK)

The responses received about the game play from the design expert (from academia) are illustrated below. Only the responses that are unique at each design are listed.

(a) Options screen

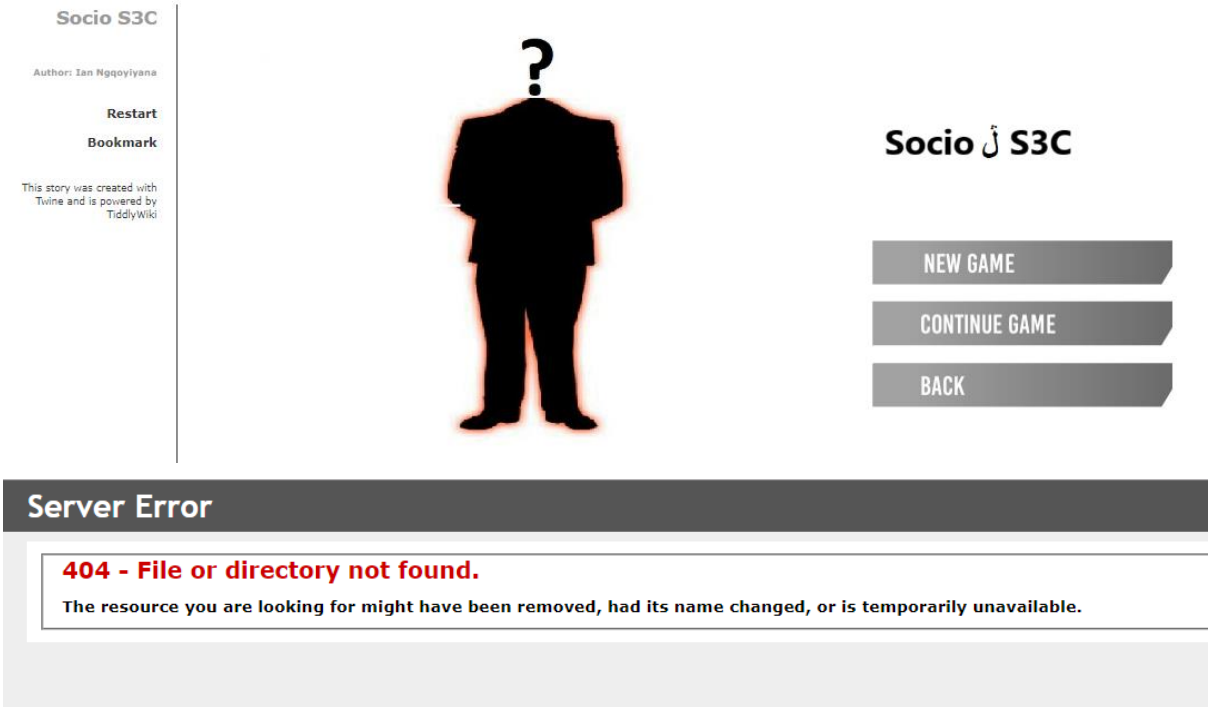
The “Sound” mute option did not work. Once clicked, it showed a message that sound is muted, but in actual fact, it is not.

Sound mute button did not work

(b) Start Screen 3

Clicking “continue game” presented a server error.

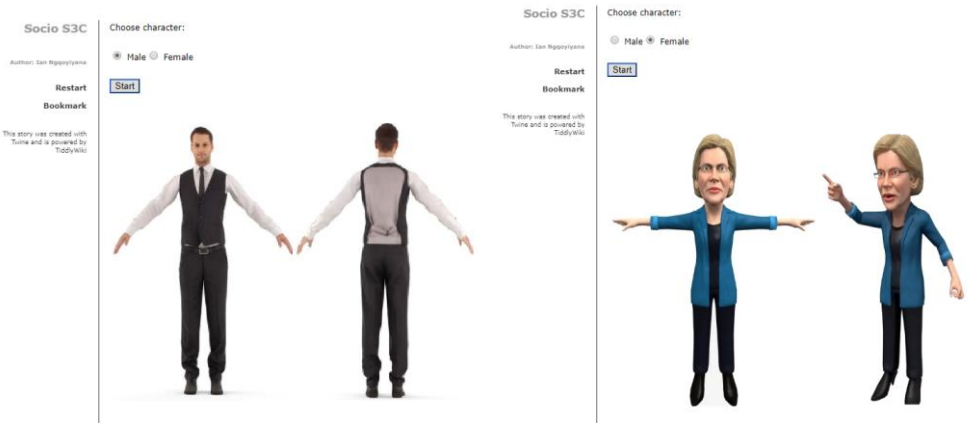
Server error when trying to continue with the game play



(c) New Game – select character

The character designs are very different from each other.

Unusually different character designs



(d) Facility screen

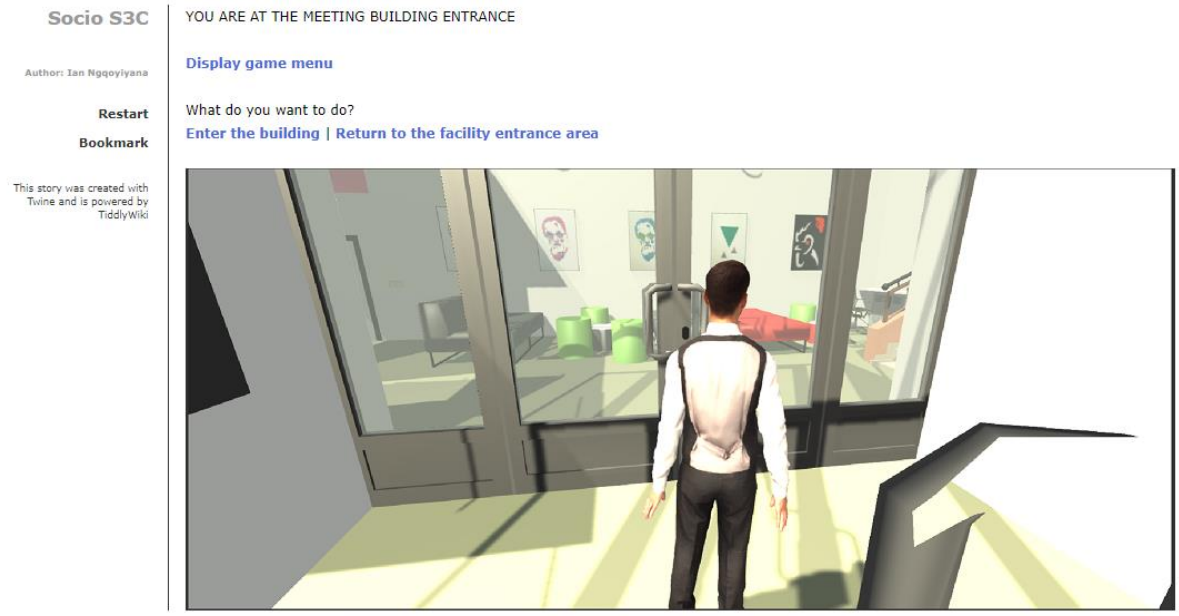
The overall interactivity of the character would have been improved if the mobility is done as a hotspot rather than text links at the top of the screen.

Hotspots for character mobility

(e) Meeting building entrance

Main game screen size and game menu screen sizes are not equivalent.

Screen sizes not equivalent



(f) Meeting room entrance

The indication of the tail gating event occurred abruptly.

Unexpected game play event

Socio S3C

Author: Ian Ngqoyiyana

Restart

Bookmark

This story was created with Twine and is powered by TiddlyWiki

YOU ARE AT THE MEETING ROOM ENTRANCE

Under normal conditions, this area is locked. It seems someone forgot to close the door!

Display game menu

What do you want to do?

Go into the meeting room | Go back and see other areas of the buidling.

Socio S3C

Author: Ian Ngqoyiyana

Restart

Bookmark

This story was created with Twine and is powered by TiddlyWiki

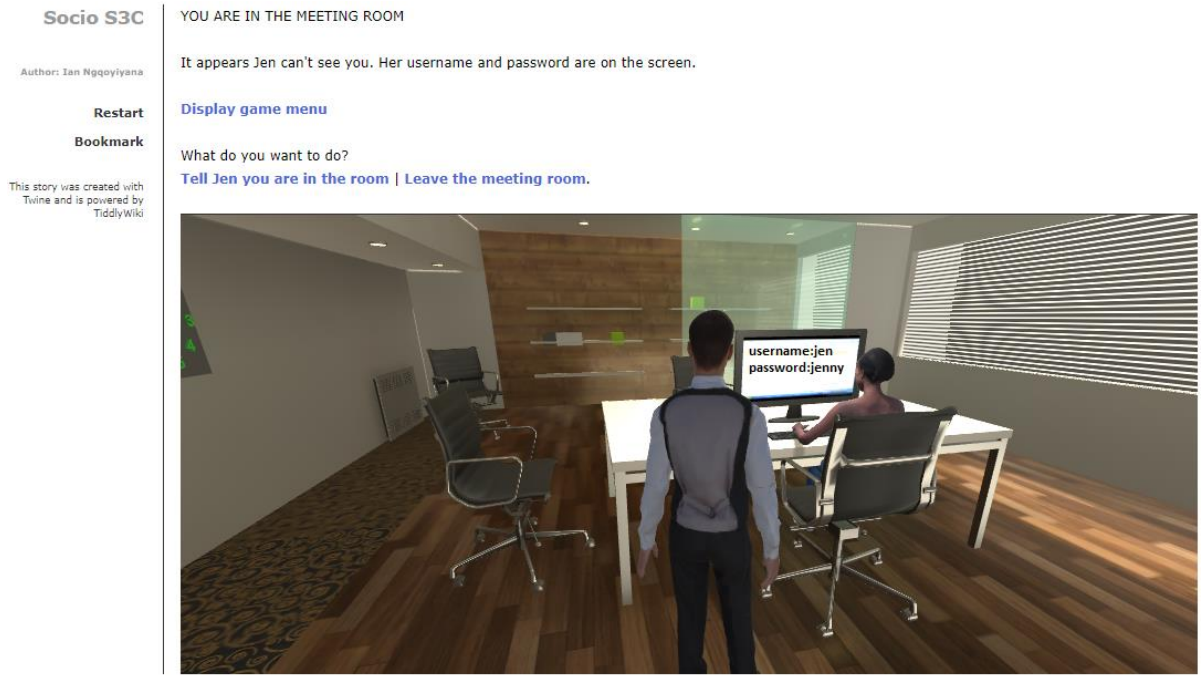
You have just used someone else's access to enter a restricted area. This is known as Tailgating.

Continue

(g) In the meeting room

There is a loose story tail whereby an audio clip plays then nothing happens.

Loose story tail



APPENDIX J: OPEN-CODED RESULTS FROM WORKSHOP 3

During the third workshop that was held mid-artefact, participants from the target user group and two cyber security professionals were presented with the first prototype. A series of questions were asked that touched on the criteria defined by Mckenney and van den Akker (2005:48). Some of the questions presented to the participants included:

- Is the game setting appropriate?
- Are the characters appropriate for the setting and game?
- Are the challenges in the game suitable for reaching the desired research objective?
- Are the character actions suitable for the game and enable you to complete the outlined challenges?
- Are you able to keep track of your progress through the game to determine where you are in the game?

The themes that were identified from the participant responses during the third workshop are presented in the table below.

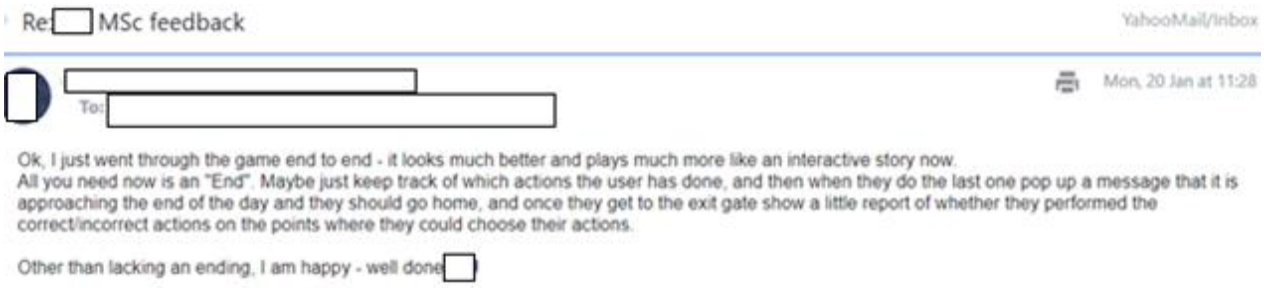
Coded summary of the key themes identified in the third requirements gathering workshop

Code	Description within context of workshop feedback
Theme 1: Platform	
Computer/laptop-based game (2 occurrences)	The game should be played on a desktop computer or laptop.
Web based (1 occurrence)	The game should be accessible over the internet on a web browser.
Theme 2: Character	
Variety in character selection (1 occurrence)	More variety in character selections, i.e. either have more characters or be able to change character appearances.
Does not care about character design (2 occurrences)	Does not really care how character appears.
Theme 3: Mechanics	
Interactivity (4 occurrences)	More interactive design with random objects.
Game should be open (1 occurrence)	Player should be able to walk around freely (externally and in the building rooms).

Code	Description within context of workshop feedback
Game should have an ending (2 occurrences)	Game should have an end-to-end storyline that tells the player that they have completed playing the game.
Introduction to game objective during gameplay (5 occurrences)	Game should provide introduction on the objective during start of gameplay.
Dumpster diving challenge should be clarified (4 occurrences)	The dumpster diving challenge is not presented clearly.
Tailgating challenge should be clarified (5 occurrences)	The tailgating challenge is not presented clearly.
Display a scoring system for wrong/right answers to questions (2 occurrences)	The game should show a scoring of wrong/right answers for challenges.
Does not care about scoring system (1 occurrence)	Does not really care about scoring system.
Videos to explain concepts (1 occurrence)	The game should have videos that explain difficult concepts to the player.
Theme 4: UI Design	
N/A	N/A

From the themes identified, it is clear that the new participants still preferred a desktop-based artefact. It is also clear that the artefact should be made more interactive as the participants indicated that it did not provide a good user experience.

APPENDIX K: PROTOTYPE 2 REVISION (REVISION 1 – EXPERT FEEDBACK)



Re: [redacted] MSc feedback

YahooMail/Inbox

[redacted]

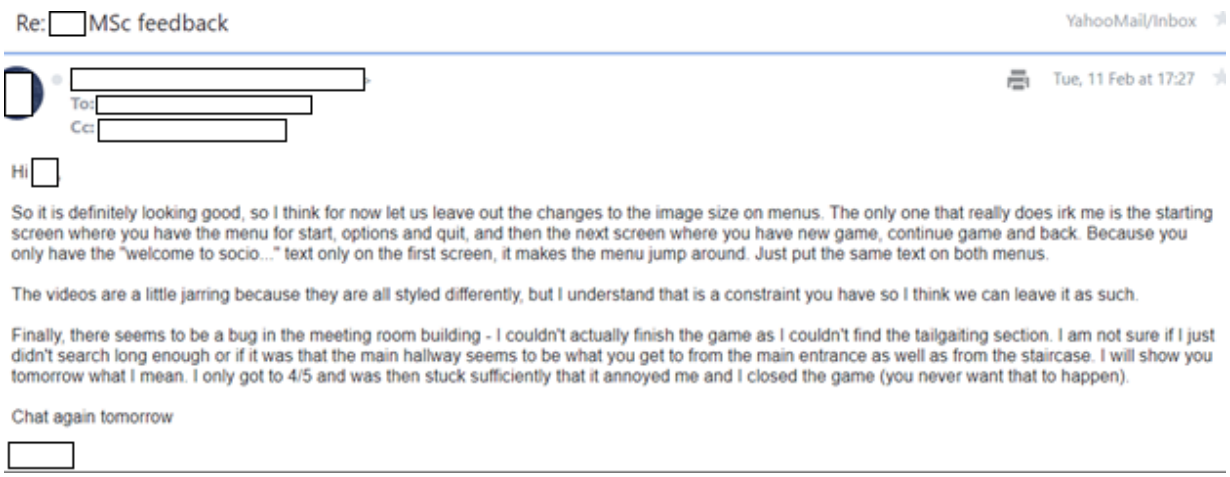
To: [redacted]

Mon, 20 Jan at 11:28

Ok, I just went through the game end to end - it looks much better and plays much more like an interactive story now.
All you need now is an "End". Maybe just keep track of which actions the user has done, and then when they do the last one pop up a message that it is approaching the end of the day and they should go home, and once they get to the exit gate show a little report of whether they performed the correct/incorrect actions on the points where they could choose their actions.

Other than lacking an ending, I am happy - well done[redacted]

APPENDIX L: PROTOTYPE 2 REVISION (REVISION 2 – EXPERT FEEDBACK)



Re: [redacted] MSc feedback

YahooMail/Inbox

[redacted]

Tue, 11 Feb at 17:27

To: [redacted]

Cc: [redacted]

Hi [redacted]

So it is definitely looking good, so I think for now let us leave out the changes to the image size on menus. The only one that really does irk me is the starting screen where you have the menu for start, options and quit, and then the next screen where you have new game, continue game and back. Because you only have the "welcome to socio..." text only on the first screen, it makes the menu jump around. Just put the same text on both menus.

The videos are a little jarring because they are all styled differently, but I understand that is a constraint you have so I think we can leave it as such.

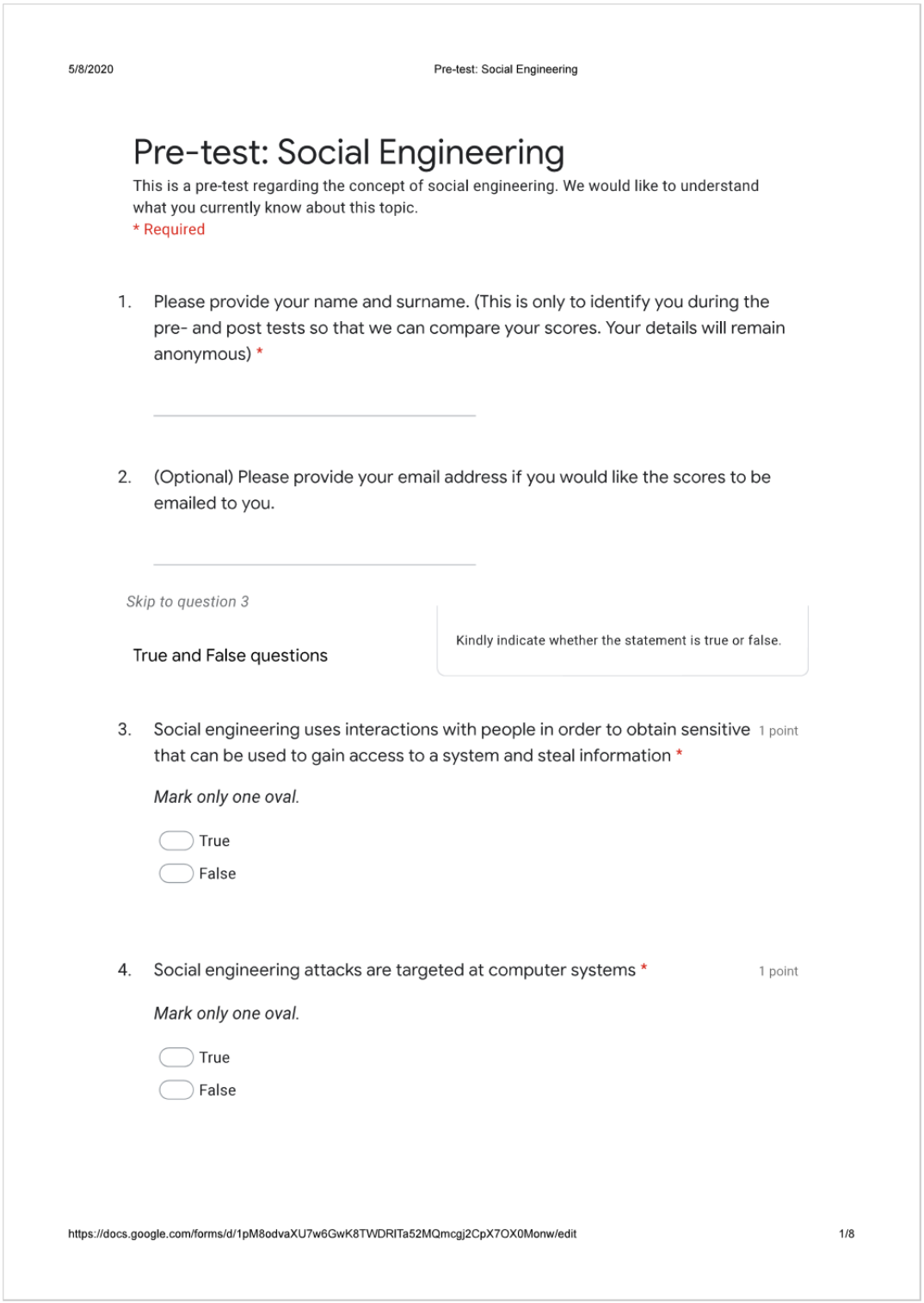
Finally, there seems to be a bug in the meeting room building - I couldn't actually finish the game as I couldn't find the tailgaiting section. I am not sure if I just didn't search long enough or if it was that the main hallway seems to be what you get to from the main entrance as well as from the staircase. I will show you tomorrow what I mean. I only got to 4/5 and was then stuck sufficiently that it annoyed me and I closed the game (you never want that to happen).

Chat again tomorrow

[redacted]

APPENDIX M: PRE-TEST QUESTIONNAIRE FORM (LEARNING EVALUATION)

The pre-test questionnaire form, which was presented to the participants before they interacted with the artefact, is presented below.



5/8/2020 Pre-test: Social Engineering

Pre-test: Social Engineering

This is a pre-test regarding the concept of social engineering. We would like to understand what you currently know about this topic.

* Required

1. Please provide your name and surname. (This is only to identify you during the pre- and post tests so that we can compare your scores. Your details will remain anonymous) *

2. (Optional) Please provide your email address if you would like the scores to be emailed to you.

Skip to question 3

True and False questions

Kindly indicate whether the statement is true or false.

3. Social engineering uses interactions with people in order to obtain sensitive that can be used to gain access to a system and steal information * 1 point

Mark only one oval.

- True
- False

4. Social engineering attacks are targeted at computer systems * 1 point

Mark only one oval.

- True
- False

https://docs.google.com/forms/d/1pM8odvaXU7w6GwK8TWDRITa52MQmcgj2CpX7OX0Monw/edit 1/8

5. Dumpster diving, or otherwise known as trashing, is a social engineering technique that is focused on an organisation's trash in order to possibly obtain sensitive information that is contained in documents that have been thrown away without being shredded correctly * 1 point

Mark only one oval.

- ◯ True
- ◯ False

6. Dumpster driving is an attack that driven by a fabrication scenario that attempts to steal personal information from a target * 1 point

Mark only one oval.

- ◯ True
- ◯ False

7. Phishing attacks occur when users click on links that redirect them to legitimate looking but malicious web sites that use fear tactics into scaring users to divulging sensitive information * 1 point

Mark only one oval.

- ◯ True
- ◯ False

8. Phishing attacks is a technique that is used to gather sensitive information by essentially looking over the victim's shoulder to obtain sensitive information * 1 point

Mark only one oval.

- ◯ True
- ◯ False

9. Baiting is a similar attack to that of a phishing attack except that it lures victims into divulging sensitive information by promising them something if they provide the information * 1 point

Mark only one oval.

- ◯ True
- ◯ False

10. Baiting entices the victim into initiating the interaction, typically by fabricating a problem for the victim and presenting a viable solution * 1 point

Mark only one oval.

- ◯ True
- ◯ False

11. Tailgating is a type of attack that occurs when the attacker gains physical access to a restricted area by impersonating a trusted entity to the victims * 1 point

Mark only one oval.

- ◯ True
- ◯ False

12. Tailgating is an attack that is commonly achieved through impersonation, where the attacker pretends to be someone the victim is familiar with and can trust them enough into divulging sensitive information * 1 point

Mark only one oval.

- ◯ True
- ◯ False

13. Water holing is a social engineering attack that requires a legitimate website (often used by the victim) to be compromised and used to obtain sensitive information from the target victim * 1 point

Mark only one oval.

- ◯ True
- ◯ False

14. Water holing refers to long-term and mostly Internet-based espionage attacks, whereby an attacker intends to maintain access to the compromised system(s) for an extended time in order to mine sensitive data * 1 point

Mark only one oval.

- ◯ True
- ◯ False

Skip to question 15

Multiple choice questions

Please choose one correct answer.

15. Which of the following is not considered a social engineering attack? * 1 point

Mark only one oval.

- ◯ Spamming
- ◯ Phishing
- ◯ Pretexting
- ◯ Tailgating

16. What is an attack that exploits human psychology? * 1 point

Mark only one oval.

- ◯ Cross site scripting (XSS)
- ◯ Social engineering
- ◯ Insecure network
- ◯ Reverse social engineering

17. What is the correct way of disposing a photocopy of your ID? * 1 point

Mark only one oval.

- ◯ Throw it in the dustbin at home
- ◯ Leave it on your office desk
- ◯ Shred it using a paper shredder
- ◯ Flush it down the toilet

18. Which of the following is a technique used to look for information inside a dustbin container? * 1 point

Mark only one oval.

- ◯ Pretexting
- ◯ Baiting
- ◯ Dumpster diving
- ◯ Quid pro quo

19. Which of the following is a legitimate Facebook domain: * 1 point

Mark only one oval.

- ◯ www.facebook.site.co.za
- ◯ www.facebook.passwordreset.com
- ◯ www.facebook.onion
- ◯ www.pictures.facebook.com

20. In a phishing attack, attackers would typically use which technology? * 1 point

Mark only one oval.

- Emails
- Wi-Fi networks
- Operating systems
- Database systems

21. Phishing can be quickly spotted by looking at which one of the following signs: * 1 point

Mark only one oval.

- The pictures in the message
- Grammar and spelling errors
- The styling of the message
- The signature of the sender

22. Which social engineering attack would typically involve picking up a USB drive that has malware loaded on it, and plugging it in to your computer? * 1 point

Mark only one oval.

- Pretexting
- Scareware
- Phishing
- Baiting

23. What should you do if you pick up a USB drive at your office door? * 1 point

Mark only one oval.

- ◯ Connect it to your computer to see what's on it
- ◯ Give it to your friend
- ◯ Report it to the security or information security office
- ◯ Take it home

24. When a person closely follows someone to gain access into a restricted area, it is often known as? * 1 point

Mark only one oval.

- ◯ Baiting
- ◯ Phishing
- ◯ Quo pro quo
- ◯ Tailgating

25. Which social engineering attack would typically involve a website that has been hacked and contains malicious code that will execute when the page loaded? * 1 point

Mark only one oval.

- ◯ Phishing
- ◯ Water holing
- ◯ Scareware
- ◯ Baiting

26. One of the main ways of preventing water holing attacks is to: * 1 point

Mark only one oval.

- ◯ Keep system vulnerability patching current
- ◯ Check your email subject line
- ◯ Not send email
- ◯ Use the Internet less

27. Which one of the following options is the most cost effective way to prevent social engineering attacks? * 1 point

Mark only one oval.

- ◯ Install an antivirus
- ◯ Ensure all patches are up to date
- ◯ Implement user awareness training
- ◯ Monitor and control email

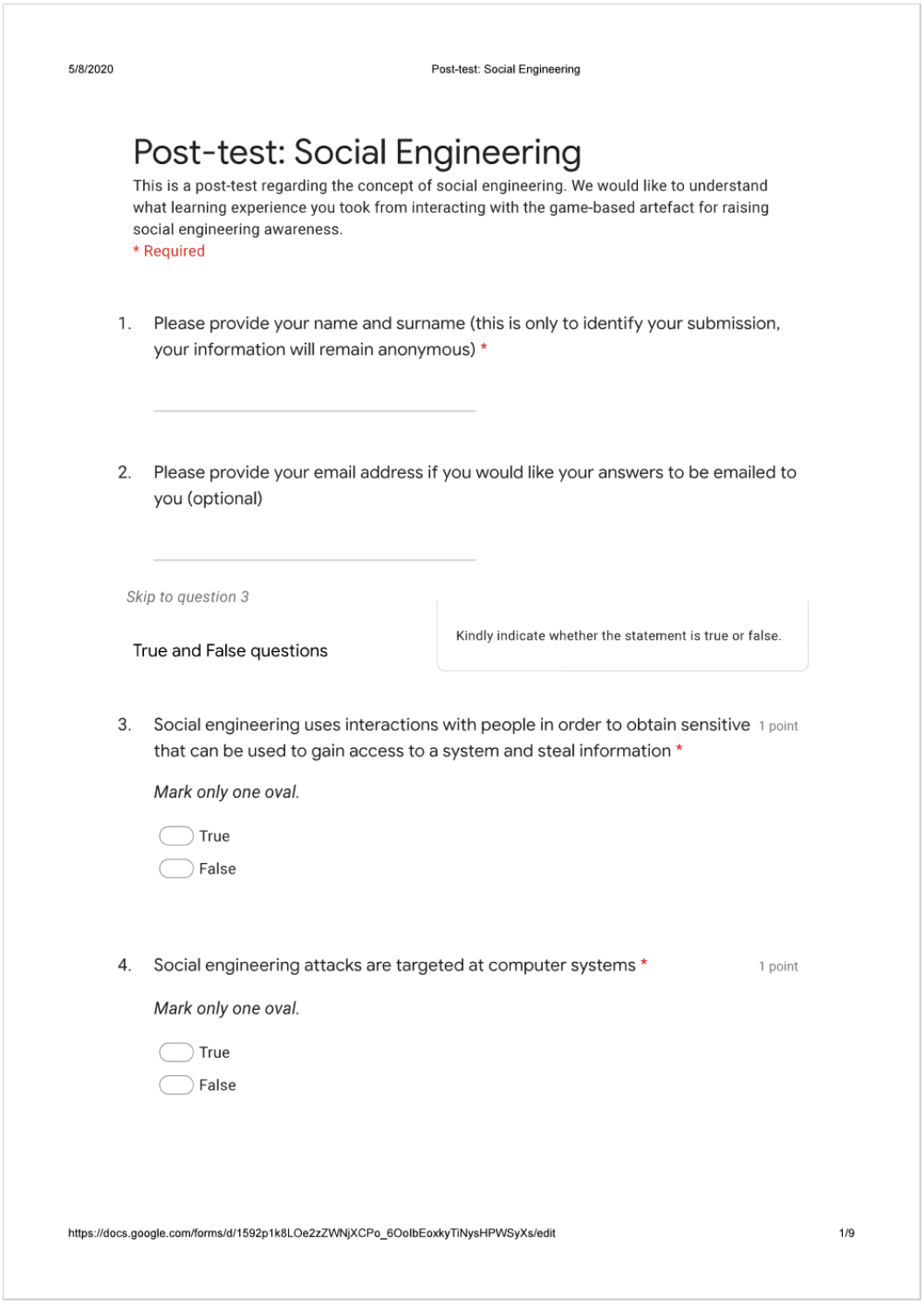
Skip to section 4 (Thank you for your time)

Thank you for your time

Thank you for completing the pre-test. You will now be introduced to a game-based artefact for raising social engineering awareness through user training.

APPENDIX N: POST-TEST QUESTIONNAIRE FORM (LEARNING EVALUATION)

The post-test questionnaire form, which was presented to the participants after they interacted with the artefact, is presented below.



5/8/2020 Post-test: Social Engineering

Post-test: Social Engineering

This is a post-test regarding the concept of social engineering. We would like to understand what learning experience you took from interacting with the game-based artefact for raising social engineering awareness.

* Required

1. Please provide your name and surname (this is only to identify your submission, your information will remain anonymous) *

2. Please provide your email address if you would like your answers to be emailed to you (optional)

Skip to question 3

True and False questions

Kindly indicate whether the statement is true or false.

3. Social engineering uses interactions with people in order to obtain sensitive that can be used to gain access to a system and steal information * 1 point

Mark only one oval.

- True
- False

4. Social engineering attacks are targeted at computer systems * 1 point

Mark only one oval.

- True
- False

https://docs.google.com/forms/d/1592p1k8LOe2zZWNjXCPo_6OoIbEoxkyTiNysHPWSyXs/edit 1/9

5. Dumpster diving, or otherwise known as trashing, is a social engineering technique that is focused on an organisation's trash in order to possibly obtain sensitive information that is contained in documents that have been thrown away without being shredded correctly * 1 point

Mark only one oval.

- ◯ True
- ◯ False

6. Dumpster driving is an attack that driven by a fabrication scenario that attempts to steal personal information from a target * 1 point

Mark only one oval.

- ◯ True
- ◯ False

7. Phishing attacks occur when users click on links that redirect them to legitimate looking but malicious web sites that use fear tactics into scaring users to divulging sensitive information * 1 point

Mark only one oval.

- ◯ True
- ◯ False

8. Phishing attacks is a technique that is used to gather sensitive information by essentially looking over the victim's shoulder to obtain sensitive information * 1 point

Mark only one oval.

- ◯ True
- ◯ False

9. Baiting is a similar attack to that of a phishing attack except that it lures victims into divulging sensitive information by promising them something if they provide the information * 1 point

Mark only one oval.

- ◯ True
- ◯ False

10. Baiting entices the victim into initiating the interaction, typically by fabricating a problem for the victim and presenting a viable solution * 1 point

Mark only one oval.

- ◯ True
- ◯ False

11. Tailgating is a type of attack that occurs when the attacker gains physical access to a restricted area by impersonating a trusted entity to the victims * 1 point

Mark only one oval.

- ◯ True
- ◯ False

12. Tailgating is an attack that is commonly achieved through impersonation, where the attacker pretends to be someone the victim is familiar with and can trust them enough into divulging sensitive information * 1 point

Mark only one oval.

- ◯ True
- ◯ False

13. Water holing is a social engineering attack that requires a legitimate website (often used by the victim) to be compromised and used to obtain sensitive information from the target victim * 1 point

Mark only one oval.

- ◯ True
- ◯ False

14. Water holing refers to long-term and mostly Internet-based espionage attacks, whereby an attacker intends to maintain access to the compromised system(s) for an extended time in order to mine sensitive data * 1 point

Mark only one oval.

- ◯ True
- ◯ False

Skip to question 15

Multiple choice questions

Please choose one correct answer.

15. Which of the following is not considered a social engineering attack? * 1 point

Mark only one oval.

- ◯ Spamming
- ◯ Phishing
- ◯ Pretexting
- ◯ Tailgating

16. What is an attack that exploits human psychology? * 1 point

Mark only one oval.

- ◯ Cross site scripting (XSS)
- ◯ Social engineering
- ◯ Insecure network
- ◯ Reverse social engineering

17. What is the correct way of disposing a photocopy of your ID? * 1 point

Mark only one oval.

- ◯ Throw it in the dustbin at home
- ◯ Leave it on your office desk
- ◯ Shred it using a paper shredder
- ◯ Flush it down the toilet

18. Which of the following is a technique used to look for information inside a dustbin container? * 1 point

Mark only one oval.

- ◯ Pretexting
- ◯ Baiting
- ◯ Dumpster diving
- ◯ Quid pro quo

19. Which of the following is a legitimate Facebook domain: * 1 point

Mark only one oval.

- ◯ www.facebook.site.co.za
- ◯ www.facebook.passwordreset.com
- ◯ www.facebook.onion
- ◯ www.pictures.facebook.com

20. In a phishing attack, attackers would typically use which technology? * 1 point

Mark only one oval.

- ◯ Emails
- ◯ Wi-Fi networks
- ◯ Operating systems
- ◯ Database systems

21. Phishing can be quickly spotted by looking at which one of the following signs: * 1 point

Mark only one oval.

- ◯ The pictures in the message
- ◯ Grammar and spelling errors
- ◯ The styling of the message
- ◯ The signature of the sender

22. Which social engineering attack would typically involve picking up a USB drive that has malware loaded on it, and plugging it in to your computer? * 1 point

Mark only one oval.

- ◯ Pretexting
- ◯ Scareware
- ◯ Phishing
- ◯ Baiting

23. What should you do if you pick up a USB drive at your office door? * 1 point

Mark only one oval.

- ◯ Connect it to your computer to see what's on it
- ◯ Give it to your friend
- ◯ Report it to the security or information security office
- ◯ Take it home

24. When a person closely follows someone to gain access into a restricted area, it is often known as? * 1 point

Mark only one oval.

- ◯ Baiting
- ◯ Phishing
- ◯ Quo pro quo
- ◯ Tailgating

25. Which social engineering attack would typically involve a website that has been hacked and contains malicious code that will execute when the page loaded? * 1 point

Mark only one oval.

- ◯ Phishing
- ◯ Water holing
- ◯ Scareware
- ◯ Baiting

26. One of the main ways of preventing water holing attacks is to: * 1 point

Mark only one oval.

- ◯ Keep system vulnerability patching current
- ◯ Check your email subject line
- ◯ Not send email
- ◯ Use the Internet less

27. Which one of the following options is the most cost effective way to prevent social engineering attacks? * 1 point

Mark only one oval.

- ◯ Install an antivirus
- ◯ Ensure all patches are up to date
- ◯ Implement user awareness training
- ◯ Monitor and control email

Skip to question 28

Comments and suggestions

28. Now that you have interacted with the game, do you have any comments or suggestions?

_____

_____

_____

_____

_____

Skip to section 5 (Thank you for your time)

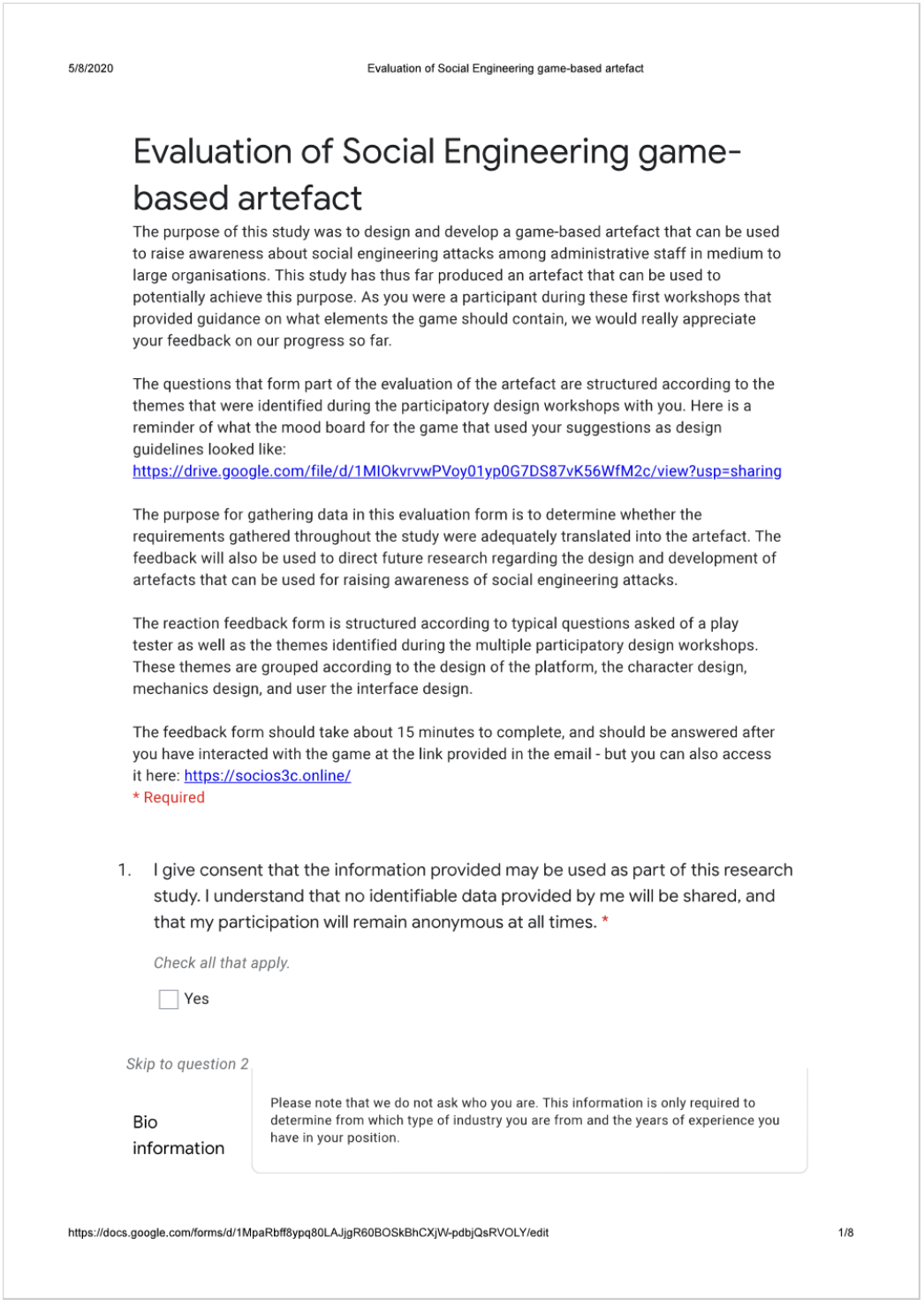
Thank you for your time

Thank you for completing the post-test. We appreciate your willingness to take part in this study.

5/8/2020 Post-test: Social Engineering

APPENDIX O: OPEN-ENDED QUESTIONNAIRE (REACTION EVALUATION)

The figure below represents the opening page the participant is presented with, which provides background to the study and obtains consent from the participant. The questions asked in the open-ended questionnaire follow below the opening page of the questionnaire form.



5/8/2020 Evaluation of Social Engineering game-based artefact

Evaluation of Social Engineering game-based artefact

The purpose of this study was to design and develop a game-based artefact that can be used to raise awareness about social engineering attacks among administrative staff in medium to large organisations. This study has thus far produced an artefact that can be used to potentially achieve this purpose. As you were a participant during these first workshops that provided guidance on what elements the game should contain, we would really appreciate your feedback on our progress so far.

The questions that form part of the evaluation of the artefact are structured according to the themes that were identified during the participatory design workshops with you. Here is a reminder of what the mood board for the game that used your suggestions as design guidelines looked like:
https://drive.google.com/file/d/1MIOkvrvwPVoy01yp0G7DS87vK56WfM2c/view?usp=sharing

The purpose for gathering data in this evaluation form is to determine whether the requirements gathered throughout the study were adequately translated into the artefact. The feedback will also be used to direct future research regarding the design and development of artefacts that can be used for raising awareness of social engineering attacks.

The reaction feedback form is structured according to typical questions asked of a play tester as well as the themes identified during the multiple participatory design workshops. These themes are grouped according to the design of the platform, the character design, mechanics design, and user the interface design.

The feedback form should take about 15 minutes to complete, and should be answered after you have interacted with the game at the link provided in the email - but you can also access it here: https://socios3c.online/
* Required

1. I give consent that the information provided may be used as part of this research study. I understand that no identifiable data provided by me will be shared, and that my participation will remain anonymous at all times. *

Check all that apply.

☐ Yes

Skip to question 2

Bio information

Please note that we do not ask who you are. This information is only required to determine from which type of industry you are from and the years of experience you have in your position.

https://docs.google.com/forms/d/1MpaRbff8ypq80LAJjgR60BOSkBhCXjW-pdbjQsRVOLY/edit 1/8

2. Type of participant *

Mark only one oval.

- ◯ Administrative/ Support role
- ◯ Cyber security professional
- ◯ Design expert

3. Year of experience in the role indicated in previous question? (e.g. 3 years/ 11 months) *

_____

4. Field of current position: *

Mark only one oval.

- ◯ Academic sector
- ◯ Industry sector

Skip to question 5

Theme 1 of 4: Platform

During the participatory design workshops – the preferred platform requirements indicated by you included the following:

- Computer/ laptop-based game – should be played on a desktop computer or laptop.
- Web-based game – should be accessible over the Internet

5. How did the game-based artefact address / not address the platform requirements? *

_____

_____

_____

_____

_____

6. How can the game be designed to better suit the platform? *

Skip to question 7

Theme 2 of 4:
Character

During participatory design workshops – the preferred character requirements included the following:

- The characters should be selectable
- Characters should closely represent real-world characters

7. How did the game-based artefact address / not address the character requirements? *

8. What did you like/ dislike about the character design? *

9. What additional design elements would make the characters more suitable? *

Skip to question 10

Theme 3 of 4: Game mechanics

During participatory design workshops – the preferred mechanic requirements included the following:

- The character should be able to walk around freely in the game world
- The game should have an objective with an ending
- There should be an introduction for the purpose of the game at the start of the game
- A scoring system should display the number of challenges completed and remaining
- Videos narrations should be used to explain difficult concepts to the player

10. How did the game-based artefact address / not address the mechanic requirements? *

11. What was the most frustrating moment or aspect of the game? *

12. What was your favourite moment or aspect of the game? *

13. Was there anything you wanted to do that you couldn't? *

14. How could the artefact mechanics have been improved? *

Skip to question 15

Theme 4 of 4: User interface design

During participatory design workshops – the preferred user interface (UI) design requirements included the following:

- The game setting should relate to the relevant industries (academia and industry)
- The UI should be easy to interact with
- The game challenges should not only be set with yes/no questions
- There should be instructions on how to play the game and hints on what actions can be performed

15. How did the game-based artefact address / not address the UI design requirements? *

16. What elements could have been added to make the UI more appropriate? *

Skip to question 17

Final thoughts

17. What did you like most about the game? *

18. What did you dislike about the game? *

19. What would you change about the game and why? *

20. What was your strategy or approach during the game? *

21. What did you learn from the game? *

22. Please share anything else you think might help us improve this game.

Skip to section 8 (Thank you - we appreciate your time!)

Thank you - we appreciate your time!

Thank you for your valuable time to complete this feedback form.
We really appreciate your input.

APPENDIX P: PROOF OF SUBMISSION (MLEARN PAPER – SUBMITTED 1 AUGUST)

Dear authors,

We received your submission to mLearn 2020 (19th World Conference on Mobile and Contextual Learning):

Authors : Ian Ngqoyiyana, Jt Janse van Rensburg and Jacob Jacobus Greeff
Title : Raising social engineering awareness through gameplay
Number : 13
Track : mLearn 2020

The submission was uploaded by Juanita Janse van Rensburg <jt.jansevanrensburg@nwu.ac.za>. You can access it via the mLearn 2020 EasyChair Web page

https://easychair.org/conferences/?conf=mlearn2020

Thank you for submitting to mLearn 2020.

Best regards,
EasyChair for mLearn 2020.