Measuring the impact of information security awareness on social networks through password cracking

by

Julius Olatunji OKESOLA

Submitted in accordance with the requirements for the degree of

Doctor of Philosophy

in

Computer Science

at the

University of South Africa

Supervisor: Professor Marthie Grobler

December 2014

DECLARATION OF AUTHENTICITY

Student number: **48948535**

I declare that "**Measuring the impact of information security awareness on social networks through password cracking"** is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

_____ _____

SIGNATURE DATE

Julius Olatunji **Okesola**

ACKNOWLEDGEMENT

With my strong passion for academics, I have always known that bagging a PhD is a must for me. However, the major motivation to undertake this study was the assurance from Prof. Segun Awonusi, the Vice Chancellor of Tai Solarin University of Education (TASUED) to place me on an ETF scholarship. Even though the ETF fund was eventually not available up till the time of writing this thesis, I will forever remain grateful to Prof. Awonusi for his invaluable inspiration.

The idea of measuring information security awareness in Social Networks (SNs) originated from my fascinating interaction with my supervisors – Prof. Elmé Smith and Prof. Marthie Grobler. Whilst thanking Prof. Abayomi Arigbabu for introducing University of South Africa (UNISA) to me, I must commend Prof. Elmarie Kritzinger for her unfailing initiatives to have selected the best supervisors in Information Security to paddle me through my study. I sincerely appreciate Prof. Grobler's prompt, insightful, clear and frank feedback; her foresight in identifying values, shortcomings and obstacles; her aptitude for putting ideas into context; her extra-ordinary attention to detail; and above everything, for being patient and understanding. She ultimately made the long process of this work a worthwhile endeavour for me to appreciate the beauty in academic research.

Writing this thesis has been a one-man-show. Nevertheless, the following individuals deserve to be acknowledged for preparing me for this rigorous and long academic pursuit. Wale Oyelami of Acumento Systems Ltd.; my colleagues at TASUED – Akeem Owoade, Oluwole Green and Folakemi Ogunbanwo; and my data analysts - Oluwatobi Olorunsola and Ayobami Ilebiyi.

Being the spouse of a graduate student is not easy. Thanks to my wife, Abiola, for coping with my unpredictable schedules, for understanding the challenges in a graduate student's life, for being the first one to hear my innovative ideas, and for her quiet wisdom and unfailing loyalty. I appreciate my children – Bolaji, Folakemi, Jibola and Olatoye for their sense of humour and amazing supports, whenever I was getting hot. You all make the world a better place for me.

Finally, I am proud to say that I have produced a PhD thesis from one of the greatest universities in the world. I have to admit that it has not always been straightforward and fun, but I persevered and finally completed it. I have learned much professionally and tend to understand myself better during these years. I, therefore, owe myself a big 'thank you' and a reserved 'congratulations'.

Lastly, I shall remain grateful to the almighty God from Whom all blessings flow and with Him all good things are possible, for crowning my efforts to make this exercise a success.

EXECUTIVE SUMMARY

Since social networks (SNs) have become a global phenomenon in almost every industry, including airlines and banking, their security has been a major concern to most stakeholders. Several security techniques have been invented towards this but information security awareness (hereafter "awareness") remains the most essential amongst all. This is because users, an important component of awareness, are a big problem on the SNs regardless of the technical security implemented. For SNs to improve on their awareness techniques or even determine the effectiveness of these security techniques, many measurement and evaluation techniques are in place to ascertain that controls are working as intended.

While some of these awareness measurement techniques are inexpensive, effective and efficient to some extent, they are all incident-driven as they are based on the occurrence of (an) incident(s). In addition, these awareness measurement techniques may not present a true reflection of awareness, since many cyber incidents are often not reported. Hence, they are generally adjudged to be post mortem and risk-permissive. These limitations are major and unacceptable in some industries such as insurance, airlines and banking, where the risk tolerance level is at its lowest.

This study therefore aims to employ a technical method to develop a non-incident statistics approach of measuring awareness efforts. Rather than evaluating the effectiveness of awareness efforts by the success of attacks or occurrence of an event, password cracking is presented and implemented to proactively measure the impacts of awareness techniques in SNs. The research encompasses the development and implementation of an SN – sOcialistOnline, the literature review of the past related works, indirect observation (available information), survey (as a questionnaire in a quiz template), and statistical analysis. Consequently, measurement of awareness efforts is shifted from detective and corrective paradigms to preventive and anticipatory paradigms, which are the preferred information security approaches going by their proactive nature.

Key words: Awareness effort, impact, measurement techniques, non-incident statistics approach, password cracking, quiz template, risk permissive, SNs, sOcialistOnline.

LIST OF PUBLICATIONS

Some parts of this thesis have been peer-reviewed and published in recognised academic journals and conference proceedings, while some others are still under review and awaiting publication. The emerging publications so far are listed below: while

PAPER I: Okesola, J.O. and Grobler, M. (2014). "Developing a Secured Social Networking Site Using Information Security Awareness Techniques". *South Africa Journal of Information Management, 16(1), 1-6.* Available online: http://www.sajim.co.za/index.php/SAJIM/article/view/607.

PAPER II: Okesola, J.O. and Grobler, M. (2014). "Measuring Information Security Awareness Efforts in Social Networking Sites – A Proactive Approach". *Proceedings of the 2014 (25th) National conference of Nigeria Computer Society (NCS) on building a knowledge-based economy in Nigeria, pp. 39-45.* Available online: http://www.ncs.org.ng/wp-content/uploads/2014/08/Knowledge-Based-Economy-2014.pdf.

PAPER III: Okesola, J.O. and Grobler, M. (2014). "An Investigation into Information Security Awareness on Social Networks in South Western Nigeria". Accepted for review in the *African Journal of Information Systems,* http://digitalcommons.kennesaw.edu/ajis/.

PAPER IV: Okesola, J.O. and Grobler, M. (2014). "Effects of Security Dimensions on Information Security Awareness Efforts in Social Networking". Submitted for publication in the *Electronic Journal of Information Systems,* http://ejise.com/issue/current.html.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SELECTED ACRONYMS

API	Application Programming Interface
AT	Activity Theory
AWARENESS	Information Security Awareness
CBT	Computer-Based Training
CEO	Chief Executive Officer
CIPPIC	Canadian Internet Policy and Public Interest Clinic
CIS	Centre for Internet Security
CISC	Criminal Intelligence Service Canada
COBIT	Control Objectives for Information Technology
ECA	Electronic Communication Act
ECT	Electronic Communication and Transaction
ENISA	European Network and Information Security Agency
EPIC	Electronic Privacy Information Centre
FISMA	Federal Information Security Management Act
FTC	Federal Trade Commission
HIPAA	Health Insurance Portability and Accountability Act
ICT	Information, Communication and Technology
IS	Information System
IT	Information Technology
KAB	Knowledge, Attitudes, and Behaviours
KPI	Key Performance Indicator
OECD	Organisation for Economic Co-operation and Development
PC	Personal Computer
PII	Personally Identifiable Information
POLA	Principle of Least Authority
POLP	Principle of Least Privilege

POPI	Protection of Personal Information
PTP	Persuasive Text Password
RCT	Rational Choice Theory
SDLC	Software Development Life Cycle
SOX	Sarbanes Oxley Act
SN	Social Network
TASUED	Tai Solarin University of Education
TRA	Theory of Reasoned Action
UAT	Users' Acceptance Test
UN	United Nations
UNISA	University of South Africa
U.K.	United Kingdom
U.S.A.	United States of America.

CHAPTER 1 INTRODUCTION

1.0 Introduction

A Social Networking service is an internet service, platform, or website, whose target is to facilitate the formation of a Social Network (SN) or social relations among those that, for instance, share interests, backgrounds, activities, or real-life connections. An SN service consists of every user's representation (referred to as a profile), his/her social links, and a range of further services. Most SN services are web-based and supply ways or resources, such as email and instant electronic messaging, for users to move over the net (Wikipedia 2012b:Internet).

Currently there are numerous popular SNs with Facebook, Twitter, LinkedIn, Myspace and Google+ being widely used worldwide (Judge 2011:5). Others include Sphere and Nexopia (Canada); Bebo, VKontakte, and Hyves (The Netherlands); Draugiem.lv (Latvia), Ask-a-peer and StudiVZ (Germany); iWiW (Hungary), Tuenti (Spain), and Nasza-Klasa (Poland); Tagged, XING, Badoo and Skyrock (parts of Europe); Orkut and Hi5 (South America and Central America); LAGbook (Africa), Mixi, Wretch, renren and Cyworld (Asia and the Pacific Islands); and Pinterest (India) amongst others (Wikipedia 2012b:Internet).

Generally speaking, SNs have become a significant technological phenomenon of this century with many of them being ranked as most-visited websites worldwide. Many SN providers have started incorporating awareness programmes for their self-protection as well as their services. Consequently, for any awareness programme to contribute and at the same time be a factor to the sphere of data security, it is necessary to own a collection of strategies to study and measure its impact (Kruger & Kearney 2005:9). This study will therefore make it possible to proactively measure the impacts of awareness on SNs.

1.1 Background to the study

Google is the most visited website in the world (Kyle 2011:Internet; Shamim 2011:Internet), however, it has been competing favourably with Facebook. A case study of the American SNs reported that in 2010, Facebook was the second biggest SN in the United States of America (U.S.A.) (HuffpostTech 2011:Internet; Kiesow 2011:Internet), and has been the centre of attention multiple times due to issues surrounding privacy. A similar survey in February and June 2011 also confirmed Facebook as the second-most-visited SN in the average country in the world (Shamim 2011:Internet), with specific statistics confirming the second-place position

in the U.S.A. and the United Kingdom (Kyle 2011:Internet). As at November 2013, Facebook has been ranked as the largest media site in the whole world (Smith 2013:Internet; Vaughan-Nichols 2013:Internet). The placement of Facebook high on the list of most visited websites confirms its growth in popularity, making it the world largest SN since 2005 (Judge 2011:5; Wikipedia 2012a:Internet) with over 1.23 billion monthly users as at February 2014 (Ross 2014:Internet).

SNs offer an opportunity to meet many friends and even complete strangers online, thereby creating privacy problems (Hopper 2010:2). The growing economic value of SNs has indeed introduced several security and privacy issues, some of which have already been addressed by researchers. For example, 95% of those surveyed in the Barracuda study of October 2011 think that it is important for SNs to do a better job of protecting the users' information against account hijacking (Judge 2011:9).

To this effect, Esma, Sebasten, and Ai (2010) introduced Privacy Watch, a privacy-enhanced SN site that fulfils the basic privacy criteria of SNs. An application programming interface (API) was proposed by Asim, Mehmet, and Abdul (2010) and implemented by SNs' providers. The API provides groupings of friends through an automated system into different social groups. Built-in applications were another proposal, made by some SNs to protect users' privacy by limiting friends who get access to users' personal information.

Many users still fail to use the social circles and the applications because of a lack of awareness or the tedious process involved when grouping friends into different classes to form a Friend List (Asim et al. 2010:1). Similarly, users often find it difficult to determine the basis of categorising friends in a meaningful way for privacy and security policies settings. This suggests that technical controls may be used to tighten access controls, but they are only part of the solution and not the total solution. Changing human behaviour on the SNs through awareness techniques is therefore essential.

1.2 Terminology used in this thesis

This section describes a number of the terms used in this research thesis. These descriptions are not scientific definitions but the author's understanding of the terms. Some of these terms are discussed in more detail later in the thesis.

1. **Asset**: Information or resources that have value to an organisation or person (BIS 2009:1).

2. **Attack**: The activities undertaken to bypass or exploit deficiencies in a system's security mechanisms. By a direct attack on a system they exploit deficiencies in the underlying algorithms, principles, or properties of a security mechanism. Indirect attacks are performed when they bypass the mechanism, or when they make the system use the mechanism incorrectly (ITU-T, 2003:44).

3. **Attacker**: An entity that carries out attacks.

4. **Attribute:** A piece of information, quality or feature that is regarded as an inherent part of an object**.**

5. **Impact:** This is the result of an information security incident, caused by a threat, which affects assets. The impact could be the destruction of certain assets, damage to the Information, Communication and Technology (ICT) system, and compromise of confidentiality, integrity, availability, non-repudiation, accountability, authenticity or reliability. Possible indirect impact includes financial losses, and the loss of market share or company image. The measurement of impact permits a balance to be made between the anticipated results of an incident and the cost of the safeguards to protect against the incident (BIS 2009:8).

6. **Incident statistics technique:** A reactive measure to evaluate the effectiveness of awareness based on the occurrence of an event or success of an attack

7. **Information security awareness (awareness):** The knowledge and attitude an individual (or members of an organisation) possesses regarding the protection of the physical and, especially, information assets of that organisation. In the information security field, experts frequently speak on users' awareness, instead of attitude and knowledge. The Information Security Forum defines awareness as "the extent to which organisational members understand the importance of information security, the level of security required by the organisation and their individual security responsibilities; and act accordingly" (ISF 2005:Internet). This definition relates awareness to both the obedience and the information security requirements.

   In the context of this work, an effective awareness programme refers to the programme that is capable of influencing the knowledge, attitude, and behaviour (section 5.6.1) of the participants and making positive changes in the security culture of an SN.

8. **Non-incident statistics technique:** A proactive technique such as password cracking or phishing e-mail that is not based on the occurrence of an event or success of an attack such as number of virus attacks, significance of audit issues, etc. The non-incident statistics approach differs from the routine security tests (such as penetrating test) going by their strengths and scope. It is a class of vulnerability assessment tool (Bace & Mell 2001:23) where technical control is used to determine the vulnerability of SNs' users.

   Even though penetration testing and vulnerability assessment and are both meant for vulnerability testing, they perform two different tasks usually with different results, within the same area of focus (Glynn 2014:1). For instance, vulnerability assessment test may identify the available vulnerabilities but it will always fail to indicate the flaws that may easily be exploited to cause damage. Meanwhile, penetration tests find exploitable flaws and measure the severity of each; it is meant to show only how damaging a flaw could be in a real attack rather than find every flaw in a system" (Glynn 2014:1). Hence the none-incident statistics aims at reporting all the weakness in the password combination of the sOcialistOnline regardless of the compensating controls in place

9. **News feed:** Column of SN user's home page that is perpetually updated to list stories from individuals and pages that such user can follow on the SN.

10. **Password cracking:** The process of attempting to guess or recover a password from stored or transmitted data to gain access to an SN, system or user's profile. This is different from password recovery through sniffing clear text, which is a subverting of system security not necessarily due to weak password but poor or no encryption (Herzog 2006:65).

11. **Penetration (or Pen) test:** The practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. The test can also be used to test an organisation's security policy compliance, its employees' awareness and the organisation's ability to identify and respond to security incidents. Pen test can be manual or automated but the main objective is to determine security weaknesses and vulnerabilities.

12. **Risk:** A probability that vulnerabilities of an asset or group of assets will be exploited by a given threat resulting to liabilities, damages or other negative occurrences and consequences (BIS 2009:4).

13. **Risk score**: In the context of this study, this refers to the probability of an SN user compromising the system.

14. **Schemas**: Self-consistent views of reality that help to ignore irrelevant information while concentrating on what appears to be important to the users.

15. **sOcialistOnline**: A new SN, purposely developed for this study.

16. **Social engineering:** An attack where someone is deceived by an individual or group of people over the phone, in person or using a computer, with a particular intention to breach some security levels professionally. It is an art of gathering information that others should not disclose and share under normal conditions taking advantage of and utilizing methods of influencing and convincing (Mataracioglu & Ozkan 2010:28).

17. **Social Networking Site (or SN):** An online website that aims to bring people together by building social relations among them to share interests, views and opinions using internet services such as email and instant messaging. An SN typically consists of several services plus the users' profiles and their links.

18. **Soft issues:** Non-technical control issues such as awareness, security policy and programmes, human and physical security, which have roles to play in data privacy.

19. **Stakeholder:** An organisation or a person who places a particular value on asset(s).

20. **Third party security application:** An additional internet program such as Internet Explorer, Java Runtime Environment (JRE) and Apple QuickTime that may interfere with the operating systems (O/S), SN and the users or stakeholders. These are programs written by individuals or companies (such as Norton and Microsoft Systems) other than the provider of the SN or O/S to work within the O/S.

21. **Threat:** Events or circumstances with a potential to violate information security through information alteration (active) such as denial of service, or unauthorised access/disclosure (passive) like password eavesdropping (ITU-T 2003:4).

22. **Vulnerability**: A flaw or weakness that could be exploited to breach the security of an asset.

1.3 Statement of research problem

Heidari (2010) isolated security threats that are specific to SNs such as identity theft, blackmailing, online and physical stalking. However, while attempting to mitigate some of these threats, some literature emphasise the importance of awareness in SNs (Adams & Sasse

1999; Brodie 2009:9-20; ENISA 2007:3-7; Hinson 2012:Internet; PriceWaterHouseCoopers 2010:Internet). Similarly, techniques for raising awareness in information communication and technology have been identified (Brodie 2009:5-8; ENISA 2007:8-13; Heidari 2010:10-16; Hinson 2012:Internet), while safety and measurement remains a focus of resilience engineering at the safety research domain (Hollnagel, Woods & Leveson 2006:5).

Deborah and Richard (2011:2) generalise that "most research on resilience engineering in the safety domain should also be applicable to the cyber security and awareness domains". This is because cyber resiliency engineering is carved out of mission assurance engineering that is majorly concerned with the improvement on SNs and cyber security through groups of resilience practices. The two approaches argue that "safety measurement is a core value and not a commodity that can be counted" (Hollnagel, Woods & Leveson 2006:5).

Therefore, for an awareness programme to be effective a set of methods was developed by the European Network and Information System Agency (ENISA) to study and measure its effect. These methods are divided into four categories based on the following measurement approaches: internal protection, attack resistance, process improvement, efficiency and effectiveness (ENISA 2008:62-64). Unfortunately, most of these techniques make use of security incident statistics that do not necessarily give a true reflection of awareness. One important reason is that many cyber victims tend not to report incidents for fear of a bad reputation or inadequate response from law enforcement in terms of information security incidents. Consequently, many researchers have discarded a security incident statistics approach as a measure of awareness (ENISA 2008:60).

In response to these problems, this study presents an approach to awareness that is not based on incident statistics. Instead of measuring the effectiveness of awareness based on the occurrence of an event or success of an attack, an effective awareness measuring technique is proposed and implemented to measure the impact of awareness on SNs through password cracking.

The **thesis statement** for this study can therefore be defined as:

A password cracker can be used to measure the effectiveness of awareness efforts on SNs.

1.4 Research questions

The research problem discussed in section 1.3 and the objectives to be highlighted in section 1.5 lead to the following primary research question:

How can technical controls be used to measure the effectiveness of awareness efforts in SNs?

This work is aimed mainly at making a contribution towards awareness effectiveness measurement. The principal issues to be addressed to achieve this aim can be defined in the form of the following secondary research questions:

1. Which metrics can be applied to measure online user behaviour in SNs?
2. Which controls are available to measure awareness?
3. Why should technical controls be explored as an option to measure awareness in SNs?
4. Can password cracker be used as technical control to measure awareness in SNs?
5. Will a quiz template be an appropriate tool for data collection on the SNs?
6. Can a technical control that is not based on incident statistics be adequate to measure the effectiveness of awareness in SNs?

1.5 Objectives

The overall aim and objective of this research project is to develop and implement a technical control, which is not based on incident statistics but efficient to proactively measure the effectiveness of awareness techniques in SNs. The aim of this research also extends to accomplish the following:

- Objective 1: Measure the impact of security dimensions, knowledge, attitude and behaviour (KAB) on awareness.
- Objective 2: Ascertain the influence of information categories (personal, family, etc.) on awareness efforts.
- Objective 3: Determine the privacy intentions of SNs users and their impacts towards improving awareness.
- Objective 4: Develop a set of preventive evaluation criteria to measure the impact of awareness on SNs.
- Objective 5: Target further user awareness training, where and when necessary.

1.6 Significance of the study

With this study, it is shown that it is possible for the SN owners to proactively measure the impact of awareness efforts on SNs. In addition, the network owners are now aware of the

prospects of using technical controls to measure awareness efforts and not only to secure the information and the SN.

1.7 Research methodology

This study addresses the research questions by doing a detailed literature study on awareness limited to SN, followed by data collection and analysis. The theories underpinning this study were identified to draw up the initial theoretical framework on which the foundation of this study is based. Consequently, the proposed SN – sOcialistOnline - and password cracker used in this study were validated by a group of SN users and experts in the field.

This methodology was followed to appreciate the extent of work already done by other researchers such as Heidari (2010), Hinson (2012) and Mataracioglu and Ozkan (2010), and also to determine if related approaches have been identified or implemented. As part of this research study, sOcialistOnline is developed by the author and launched over the internet. The inherent insecurity of the SN is averted by the implementation of technical controls as well as the application of awareness techniques. As will be discussed later in section 6.3.2, the naming and capitalisation of sOcialistOnline is arbitrary, and was the author's exclusive idea with no specific basis.

1.8 Ethical consideration and due diligence

This study addresses ethical clearance and due diligence in four ways as follows:

1. The author sought and obtained a formal ethical clearance (appendix A) from the Research and Ethics Committee of College of Science and Technology (CSET), the University of South Africa (UNISA).

2. Involvement of participants throughout the study is optional, voluntary and could be anonymous. The confidentiality of information provided by them is absolutely guaranteed, and this is explicitly stated in appendices B, C, and D.

3. The aims and objectives of the awareness presentation and Users' Acceptance Test (UAT) were made clear to the intending participants through appendices B and C respectively, and each participant was urged to sign a consent form in appendix C.

4. The author subjected the thesis document to language editing to ensure that it is linguistically and technically correct by eliminating avoidable grammatical and spelling

errors. Appendix I is the copy of a certificate letter from a qualified English language editor that edited and proofread the document.

1.9 Effects of the study

This study illustrates that technical controls are not only used to secure SNs, but also to measure the effectiveness of awareness efforts in SNs. Most of the current metrics that are applicable to measure awareness in SNs are reactive rather than proactive. These metrics are post mortem because the SNs owners must wait for the occurrence of (an) event(s) or success of an attack(s) such as the number and cost of security incidents, and the scan results for unauthorised software before their (metric) effectiveness can be measured.

This work will be especially relevant to banks and airlines, where the risk tolerance level is very low. Following obtaining users' consent through the SN portals, a random sample of user passwords strengths can be analysed and a report be generated on the security league. This report can be thoroughly reviewed and presented to the management of the organisation to ensure that users are following the security policy. This will also encourage people to improve on their password combination strength. The results can also be used to plan for further awareness training if need be.

The study will illustrate the SN possibilities of being adequately protected without necessarily employing a third-party security application. Consequently, awareness effectiveness in SNs will easily be measured using a proactive approach.

1.10 Study limitations

There are two limitations that will be discussed in this section – the research overview and the implementation platform.

1.10.1 Research overview

Getting technical access to any established SN such as Facebook for research purposes is difficult. Notwithstanding, the author made some attempts to obtain access but with no success as the SN's owners could not authorise the administrative access for fear of attack and abuse. Having waited for weeks with no response to his access request, the author visited the Nigerian offices of the country managers of Google and Facebook in Lagos. They individually declined the request asserting that giving access to their networks for academic research is against their

operational policy. This study is, therefore, restricted to sOcialistOnline - the SN developed by the author.

However, to eliminate the possibility for bias and challenges with replication and to make the research approach acceptable to UNISA, sOcialistOnline is subjected to the same requirements, environmental and technical factors as Facebook and other SNs. Although sOcialistOnline supports third party connection and can interface seamlessly, the use of such applications to secure the SN is discouraged in order to guard the SN against potential third party application threats. Similarly, the unit test is limited to the postulated model and the conclusion is based on the evaluation of the data obtained.

This limitation negatively affected the research time, cost, and the volume of primary data obtained. Subsequently, the developed SN experienced low users' patronage because it was new and not yet popular, thereby necessitating the need to extend the initial research period to capture more data. Notwithstanding, this limitation did not have any effect on the scientific validity of the study, since it was mitigated by adequate funding and an extended research period.

1.10.2 Implementation platform

The solution to the research problem is the implementation of the author's own SNs - sOcialistOnline, on the internet. The implementation is platform independent and thereby has no limitation to a particular environment. However, the author concentrated on the academic environment because that is where enough primary data can easily be obtained, since students/youths are more inclined to use SNs. Similarly, it is postulated that the academic environment has a very high risk tolerance level, and security is not given a top priority since the impact of an attack is not regarded as severe as an attack in the airline or banking environment.

Although the study results may be skewed since 95% of the sample used in this study is students, it could also be an advantage because students are more experienced SN users and generally technology inclined. They tend to post more potential sensitive information on the SNs when compared to an older target audience. Furthermore, since students will soon be in the job market, it is expected that they will be more security-conscious and that the correct use of privacy settings would be more important to them.

1.11 Chapters overview

This section presents an overview, in a tabular form, of all the chapters in this study. It uses table 1 to outline each chapter title against its respective research questions/objectives and output.

Table 1: Chapter overview (own compilation)

Chapter #	Chapter title	Research question/ Objective addressed	Output
1.	Introduction	All research questions.	Thesis statement, research problems, aims and objectives are defined and stated.
2.	Methodology of research study	All research objectives.	The research methodology employed and the phases of the study are summarised towards achieving the research objectives.
3.	Related works	All research questions.	Overview and theoretical foundation for the research questions are provided.
4.	Rationales for awareness in SNs	Research question 2, objectives 1, and 2.	Needs to measure awareness in SNs is justified.
5.	Awareness measurement in SNs	Research questions 2, 3 and 4; and research objective 1.	A proactive approach is considered the best method to measure awareness efforts.
6.	The sOcialistOnline	Research questions 1, 2, 3, 4, and 6.	A safe SN is developed and implemented online real-time.
7.	Data-gathering and awareness measurement	Overall objective, primary research question and research questions 2, 4, 5 and 6.	Relevant research data are gathered, and awareness efforts are measured using an approach that is not based on incident statistics.
8.	Findings and discussion	All the research objectives.	The findings are validated to authenticate how the research objectives are met.
9.	Reflection and conclusion	All the research questions and objectives.	The entire study is summarised, reflected on and conclusions are drawn with recommendations for future study.

1.12 Summary

Many security incidents are born out of unsafe user behaviour and the basic security exposures in technology of the SNs. However, as will be established by this study, most of those unsafe acts are attributable to the lack of adequate user awareness. A key issue here is foresight – the ability to anticipate potential risks before failure and damage happen. As such, this study will address the use of a password cracker to measure the impact of awareness on SNs proactively. It will be in a clear distinction to the standard reactive approach driven by events that have already happened.

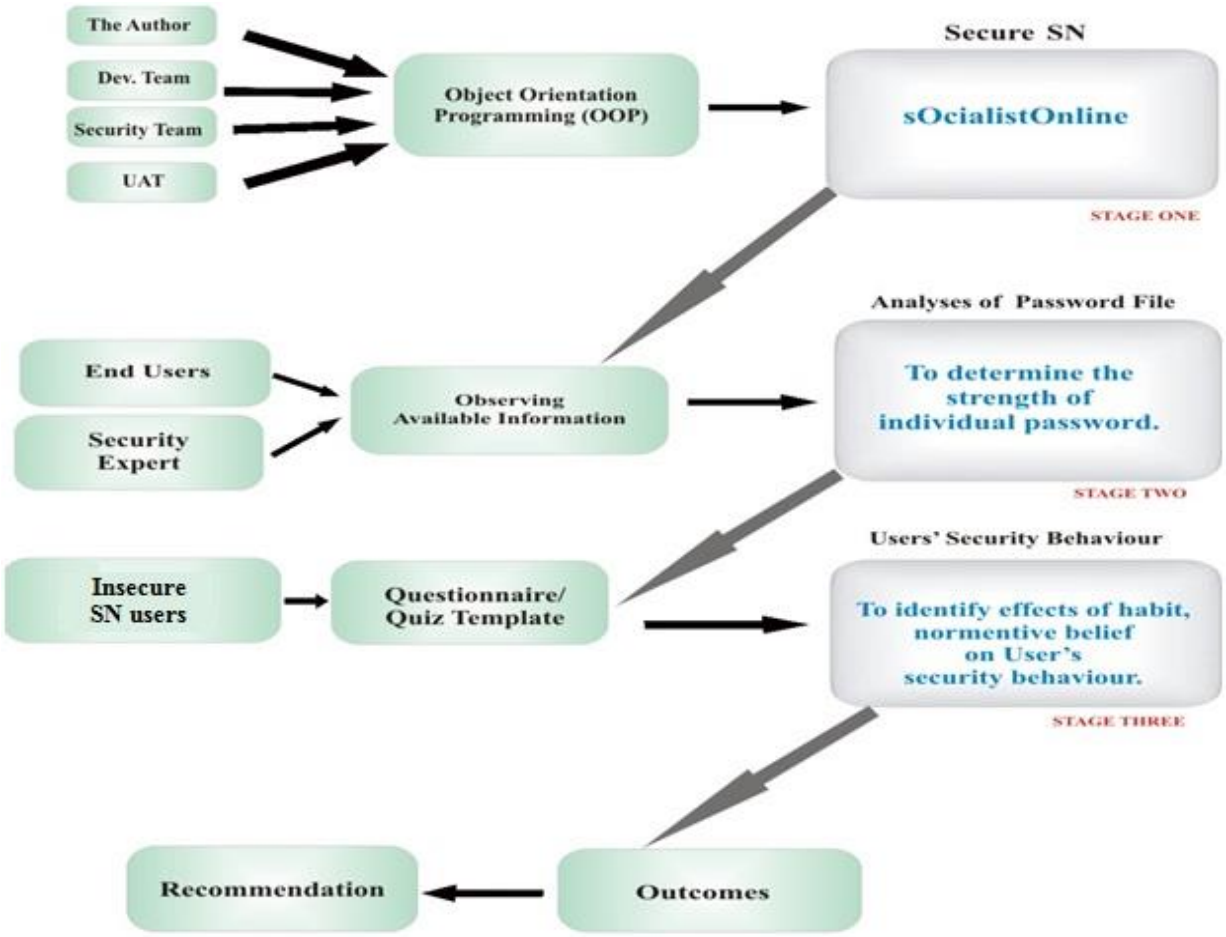
To pursue the thesis statement that the effectiveness of awareness efforts on SNs can better be measured before the occurrences of events, this chapter presented a brief introduction into SN safety and measurement. These descriptions are not scientific definitions but the author's understanding of the terms. This chapter established research problems to identify the thesis statement and research objectives that led to the research questions. The author acknowledged the scientific contribution and the potential challenges of this study. The research methodology to be deployed in this work was also summarised and will be discussed extensively in the next chapter.

CHAPTER 2 METHODOLOGY OF RESEARCH STUDY

2.1 Introduction

This chapter will explain the methodology used in the research study as illustrated in figure 1. This figure exhibits various stages to describe what takes place in each of the research phases (later discussed in section 2.6). As will be discussed in Chapter 6 and 7, the overall aim of this methodology is to implement the technical control, password cracking technology, to proactively measure the awareness efforts on an SN. This study is divided into three stages, with each stage using a different research method. The stages are preceded by a comprehensive literature study of the past related works (Chapter 3) from which each of the stages is developed. The stages are interdependent as each stage is built on the results of the previous stage. The research phases as related to various research stages in this study are further discussed later in section 2.6.

Figure 1: The stages of this study (own compilation)



The major parts of the first and second stages were conducted in Lagos, Nigeria at Acumento Software laboratory due to the availability of the required software (PhP 5.3.8 and MySQL), expert knowledge, and a strong software development team. Summit Technology Nig. Limited assisted in securing the SN on the web while UAT was done at the Tai Solarin University of Education (TASUED) Ijebu-ode – Nigeria. The last stage was largely performed at the TASUED e-learning centre and ICT directorate.

The rest of this chapter is organised as follows: Section 2.2 discusses the research strategy in general, while section 2.3 presents the initial theoretical framework. The referent theories on guiding this study are highlighted in section 2.4, and the different methodological approaches employed to achieve the research objectives are presented in section 2.5. Section 2.6 presents an overview of the research phases and how the research stages are implemented in these phases. Finally, section 2.7 summarises this chapter.

2.2 Research strategy

A research strategy generally proffers a plan for a research study and ensures that appropriate methodologies are employed to address research questions (Al-Awadi 2009:49). However, in line with Carr (1994:716), a researcher is not bound to stick to an approach even though such approach has been selected. Since the nature of the findings and required data types dictates the data collection methods to be used, each approach is bound to come with its strengths and weaknesses, with each principally suitable for a particular circumstance. The research approach to be adopted in any study should therefore be a function of the research problems, as well as the goals and objectives of the researcher himself (Carr 1994:717).

There are many strategies available to carry out research studies. Creswell (2003:14-15) classifies the strategies associated with research methods are either qualitative or quantitative. Hence for reasons to be explained in section 2.5, the author resolves to utilise a hybrid method which is the combination of the two methodological approaches to drive the goals and objectives of this study.

2.3 Initial theoretical framework

Sekaran and Bougie (2010:18) define a theoretical framework as the foundation on which a study is based. They argue that "the relationship between the literature review and the theoretical framework is that the former provides a solid foundation for developing the latter". It is therefore recommended that a theoretical framework should have the following three basic features (Sekaran and Bougie 2010:18):

- Definition of variables considered relevant to the study.
- A conceptual model that describes the relationships between the variables.
- A clear explanation why these relationships are expected to exist.

The following sections will relate these features to the study.

2.3.1 Relevant variables to this study

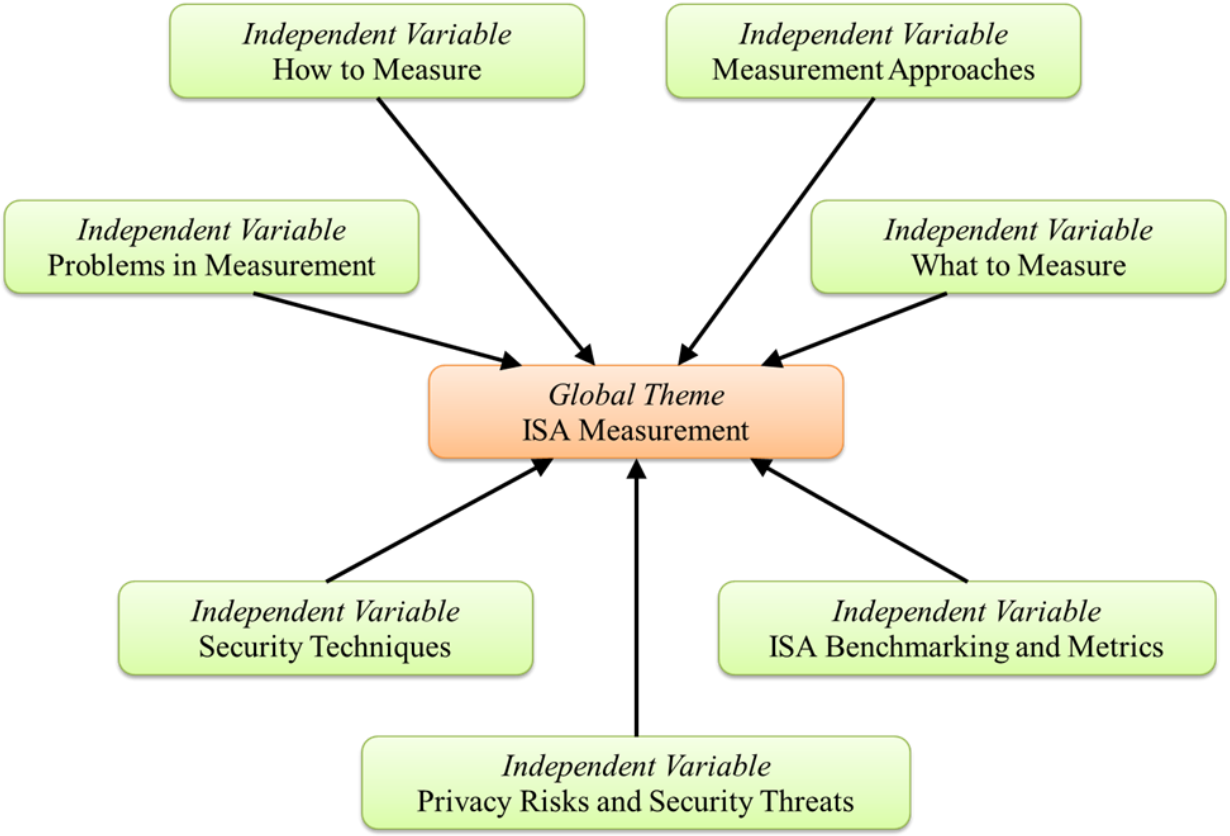
ENISA (2008:63) recommends that an information security programme of any organisations (including SNs) cannot be improved upon if the effectiveness of their implemented awareness techniques is not adequately measured. Since the subject being studied is the measurement of awareness techniques using an approach that is not based on incident statistics, this thesis focuses on awareness measurement as a global theme for this study. This global theme is a dependent variable as the measurement of awareness is dependent on so many factors, some of which are independent variables for this study.

The independent variables considered relevant to this study include: privacy risks and security threats, security techniques, measurement techniques/approaches, problems in measurement, what to measure, how to measure, and awareness benchmarking and metrics. Although the global theme (awareness measurement) is dependent on independent variables in this study, the latter is independent of any factor. These themes or variables will be defined in chapters 3, 4, and 5.

2.3.2 The conceptual model relating the variables

The conceptual model that relates both the dependent and independent variables, which influence security awareness measurement in this study, is provided in figure 2.

Figure 2: Initial framework for measuring awareness (own compilation)



2.3.3 Claims for the expected relationship to exist

As will be investigated in chapter 3, the past related works reviewed recognises privacy risks and security threats, comprising cyber-attacks and users identity threats, as factors to be curtailed by the privacy approach when raising awareness (sections 3.4.1 and 3.4.2). Security techniques as well as available measurement approaches are also identified as potential factors influencing awareness measurement, and are therefore considered as independent variables in this study.

Similarly, literature findings in chapter 5 point to the possible influence of what to measure, how to measure, awareness benchmarking and metrics, determinant factors, and problems in measuring the effectiveness of awareness efforts. These factors are the themes or relevant variables, some of which are further analysed in the empirical part of this study discussed in chapters 8 and 9.

2.4 The referent theories

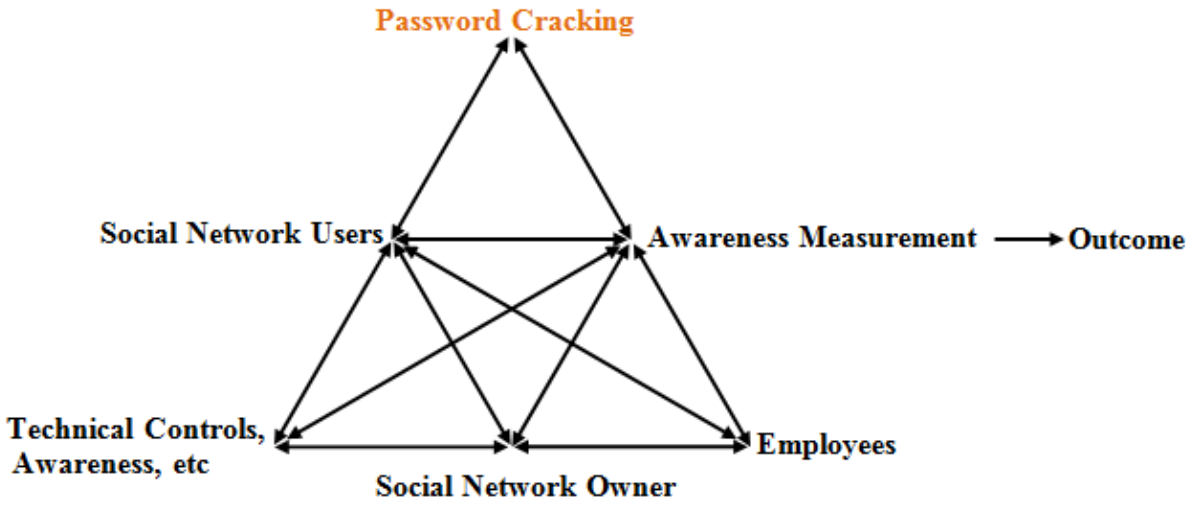
The referent theories for this study are the Markus's three theories as presented by Myers and Avison (2002), namely: system-determined, interaction-determined and people-determined.

This research on measuring awareness efforts in SN is based on the concepts from dissimilar models applied to the field of information security and human behaviour, namely: activity theory (AT), knowledge, attitude and behaviour (KAB), theory of reasoned action (TRA), and rational choice theory (RTC).

Hashim and Jones (2007) employed AT to investigate students' response to information security on their learning system and suggest that AT theory is applicable to human beings and their technological environment. Similarly, the users' KAB must be in line with the security requirement for the SN to be adequately secured (Lacey 2009:11). However, since the required changes in security behaviour on SN may not be easily attained using the KAB model alone (section 3.3.4), the combination of both the AT theory and KAB model is used to guide this study.

The general overview of the KAB model and AT is provided in chapter 3. However, figure 3 illustrates the AT model as applicable to this study.

Figure 3: Activity theory for this study (own compilation)



Relating the AT model as postulated by Engetrom (1987:77) and later described in figure 6 in section 3.3.3, the subjects are 'SN users' who are affected by the technical security on the network and are also expected to radiate secured behaviour and attitude. The object is the 'awareness measurement', which is the activity under study, and the tool or instrument is the 'password cracking', which is the approach that is not based on incident statistics, developed to proactively measure the awareness efforts in SNs. The community is the 'SN's owner' who implemented rules ('technical controls', 'privacy policy', 'awareness', etc.), while the division

of labour refers to the 'employees' of the SN who are saddled with segregation of duties for effective internal security on the SN.

2.5 Research methods used in this study

No research approach is perfect as quantitative and qualitative methods have their own individual strengths and weaknesses (Rich & Ginsburg, 1999:371). Therefore, the mixed approach gives better results in terms of quality and scope (Fryer 1991:8). For this reason, the principle of triangulation is employed in this study and it is generally based on both the interpretative and the positivistic paradigms so as to provide a balance of strengths and avoid overlapping weaknesses of the interpretative and the positivistic. The positivistic paradigm is traditional and quantitative in nature, and its main concerns are that measurement is reliable, valid, and generalizable in its clear prediction of cause and effect (Cassell & Symon 1994:2), whereas qualitative research, which is naturally interpretative, is concerned with deeds of attempting to accurately interpret and portray phenomena that normally occur in their social contexts (Fryer 1991:3-6).

Triangulation is the combination of both qualitative and quantitative approaches in research findings, and it is highly recommended by both Carr (1994) and Creswell (2003). This approach has been in use by the researchers for various research investigations. Rainer, Synder, and Carr (1991), for instance, combined qualitative and quantitative approaches to evaluate the process of risk analysis in Information System (IS). Fulford and Doherty (2003) equally administered questionnaires to investigate the application of information security policies in organisations that are based in the U.K., but they realised a need to interpret the same field with qualitative studies. In a similar work, Meister and Biermann (2008) use interviewing followed by a questionnaire to determine success in the development of application software.

The combination approach is the most appropriate for this study because the proposed solution integrates both qualitative and quantitative techniques – password cracking. Password cracker is used to automate the observation process and, therefore, presents a useful direct quantitative measure of user behaviours (ENISA 2010:94). Similarly, survey/questionnaire (quiz templates), which is one of the data collection techniques deployed, is a quantitative research method, while observation generates mainly qualitative data, even though the survey/questionnaire data is just a supplement to the study and not the integral aspect of data collection. Definitely, the analysis and understanding of this data could only be achieved by

using both the quantitative and qualitative approaches. These approaches are explained as follows and include the literature review, observation, survey, and statistical analysis.

2.5.1 Literature review

The goal of literature review is to highlight the main definitions, theories, models and empirical findings that provide background to the research questions. This implies that the literature review is meant to provide the theoretical foundation for the research in question. The literature overview, as will be presented in Chapter 3, reviews the existing related works on awareness as related to SNs (sections 3.4 - 3.6). The overview addresses all the research questions and provides the theoretical foundation for the sub-questions highlighted. It is on this basis that the initial study is planned and delimited. Consequently, the overall findings will be used to assess the contribution of this work to the scientific body of knowledge.

2.5.2 Observation

Observation is an evaluation method where users are observed while interacting with the target application (Adebesin 2011:56). Observing users on SNs is known to reveal unexpected findings, which may eventually be fed back into the newer version of the application (Preece, Rogers & Sharp 2007:8). Observation on its own cannot be sufficient to measure the effectiveness of awareness techniques on SNs because it is often difficult to understand the rationale behind the behaviour of SN users. For this reason and beliefs that some users still use guessable passwords despite their high level of awareness, an additional tool is needed for effective measurement. This study, therefore, provides additional tools – a table of profile groups and a questionnaire (quiz template) – to some categories of users, as will be discussed later in section 7.4.

In a natural setting, a researcher can ordinarily perform an observation in a controlled environment or as a component of another evaluation method (Preece et al. 2007:5), in which case, observation may be direct or indirect as discussed below.

2.5.2.1 Direct observation

Many researchers prefer systematic, direct observation of behaviour as the most accurate and desirable method of measuring the effectiveness of awareness. Using direct observation, the investigator observes and records the behaviours of the participants rather than relying on reports from supervisors or systems.

In this case, the researcher may choose to participate directly (as an insider) or be a passive observer and act as a stand-alone outsider. As an insider, he experiences the observation directly but as an outsider, he observes the user while carrying out the normal or routine activities. Direct observation can reveal details that are difficult to obtain when using other evaluation methods, as it enables the researcher to see the context of use of the application (Adebesin 2011:56). At the same time, it can be difficult due to constant environmental interruptions, and the generation of unstructured and mostly irrelevant data, which are difficult to analyse.

2.5.2.2 Indirect observation

Indirect observation is observation where user activities are recorded for later review. It is observation where the researcher depends on the report of others. This method is mostly used when the observer, for whatever reason, cannot be available at the location of the observation. Recording may be manual or automated. For example, a system controller may make use of diaries to record the uptime and downtime of a system, as well as keeping the system availability details. Interactive logging is another example in which a software application captures user activities such as logon duration and key press for later review. The attraction to this technique is that it is inexpensive and may not require special skill or equipment. However, the participants may fail to document some important information, or may exaggerate the occurrence of certain events.

Indirect observation is employed in this study, using available information/existing materials (section 7.2) already captured on the newly developed SN, sOcialistOnline. When launched on the internet, the SN keeps users' personal and confidential data, including passwords and photographs. For the fact that the key element in password security is the crackability of a password combination (Adams & Sasse 1999:41), the author's solution is aimed to crack the password files and, subsequently, analyse the individual password strength. The number of users using easily guessable passwords is a key indicator of awareness (ENISA 2008:62).

2.5.3 Survey

Surveys are conducted by means of an interview or by administering a questionnaire on a sample or even the entire population (Olivier 2004:8; Roode 2009:5). Surveys can be interviewer-administered (personal) or self-administered, telephonic or online, which includes email, computer-direct, and web-based variations (Field 2005:11). Questionnaires may come in different forms and are used for dissimilar findings in varying situations with many different

data-gathering media (Brace 2004:2). They are not always required for a survey but they do provide a standardised interview across all subjects (Olivier 2004:6).

Information-gathering by survey could be either qualitative or quantitative (Van Biljon 2006:101). For instance, when a large amount of quality data is collected from a few test participants during the interview exercise, the process is called qualitative information-gathering. However, quantitative information-gathering occurs when dynamic adaptation is impossible and a survey has to be conducted with a fixed-response questionnaire such that responses are collected from a bigger class size of respondents (Van Biljon 2006:101). The latter case is what is employed in this study where a survey is conducted in two phases – KAB privacy and intention-gathering (sections 7.4.1 and 7.4.2). In this case, questionnaire is administered in a quiz form to involve as many participants as possible since a certain number is required for statistical analyses.

2.5.3.1. Questionnaires

A questionnaire is a data collection technique where respondents are required to respond to the same set of questions in a predetermined order. In this study, an electronic questionnaire is transposed to a quiz template for easy administration, and to attract the targeted audience. A questionnaire can be administered through a computer or paper-and-pencil, and could be likened to interviewing, considering the closed or opened nature of the questions. However, it is not flexible like interviews because its questions are static, making it difficult to probe further.

Questionnaires can be a very useful and convenient means of collecting large volumes of data while respondents remain potentially anonymous. The questionnaire can be completed at the respondents' convenience without error, but it is often difficult to record a high response rate (Brace 2004:10). Creswell (2003:21), therefore, came up with a follow-up approach to avoid such situations, by monitoring phone calls and sending emails as a reminder. Brace (2004:12) admits that there are different types of questionnaires, which can be either interviewer-administered or self-administered.

Interviewer-administered questionnaires include the following:

1. Telephone questionnaires, where questionnaires are administered over the telephone.
2. Structured interviews, where an interviewer does not move away from the questions, rather he meets the respondents face-to-face.

Self-administered questionnaires include the following:

1. Postal questionnaires, in which case the distribution of the questionnaire between the researcher and the respondents is done by post.
2. Delivery and collection questionnaires, where both the delivery and collection of the questionnaire are done by hand.
3. Online questionnaires as employed in this study, where electronic mail or other online media is used to disseminate the questionnaire in a quiz format (section 7.4).

2.5.4 Statistical analysis

Using a quantitative research method, statistical analysis is often employed to analyse research results and findings. Field (2005:4) classifies statistics into only two groups – descriptive and inferential. Descriptive statistics use numeric values to describe the entire population, while inferential statistics present a mean to predict and explain certain characteristics of the individual studied (Van Biljon 2006:102). Similarly, descriptive statistics could be derived from the features of the sample, group or the entire population, thereby giving room for the researcher to describe the group (Olivier 2004:10); whereas inferential statistics are used to determine the true position of experimental hypothesis regarding the search, and also to extract the trends statistics that qualitative analysis cannot clearly offer (Field 2005:6).

It may be intimidating to select appropriate methods for statistical analyses (Van Biljon 2006:102). However, basic guides are now available to select statistical tests based on data category (normal, ordinal, or interval/ratio data), and the groups (independent or match) that the researcher is comparing and contrasting (Field 2005:7).

Since qualitative and quantitative statistical approaches were deployed in this study, both inferential and descriptive statistics were used for data analysis. Inferential statistics was employed to formulate a password analyser (section 7.2.1) by obtaining its input data from password cracker (observation), while descriptive statistics was used to analyse responses obtained from questionnaire administration (section 7.4.1). Following the cracking of users' password files, the proposed solution analyses the strength of individual passwords using an automated inferential statistical approach, while a high-level program was also developed to descriptively analyse and score data obtained from the quiz template. This is used to obtain the awareness level of each user and serves as an approach of encouraging further interests in the values and risks of using SNs, without basing it on incident statistics.

2.6 Research design

This research is performed in three stages (figure 1) but was conducted in phases. As indicated in figure 4 and summarised in table 2, there are five major phases with the findings of one phase being the input to the next. This linkage is also illustrated in figure 5 and discussed later in this section.

Figure 4: Research phases in this study (own compilation)

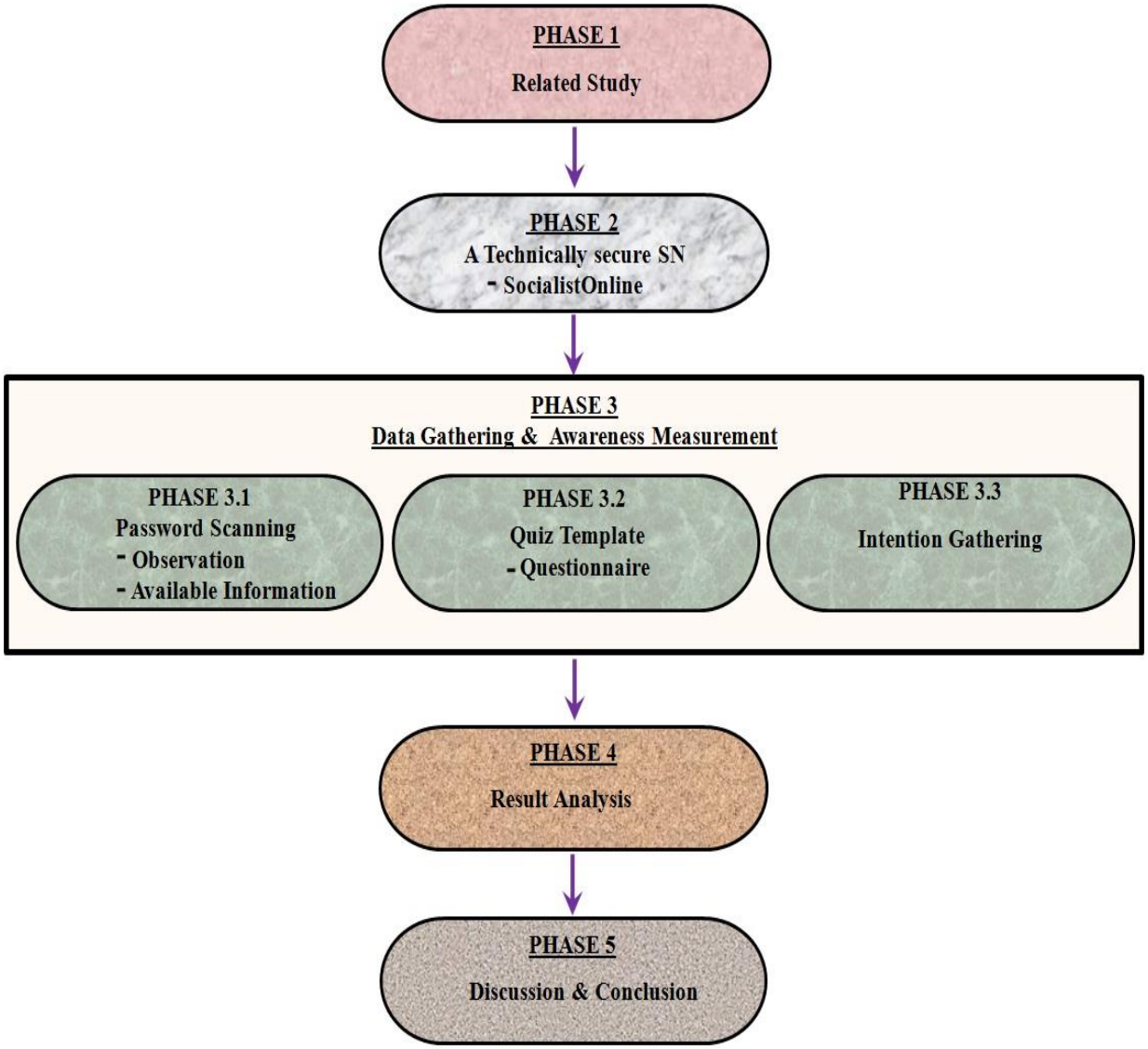
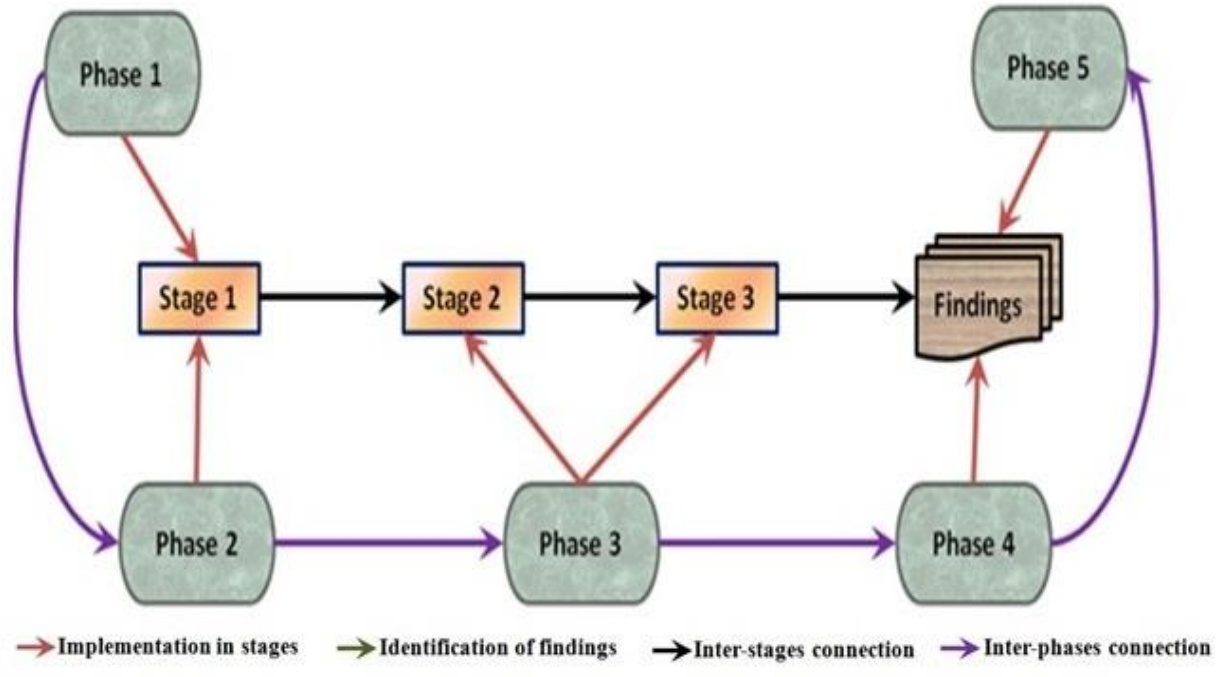


Table 2: Research phases and corresponding chapters (own compilation)

Phases	Description	Chapter(s)	Output
1	Related study	3	Identification of research questions
2	sOcialistOnline	6	A secure SN
3	Data gathering and awareness measurement	7	Password cracker, quiz template, and intention gathering table
4	Findings and discussions	8	Research findings
5.	Reflection and conclusion	8 and 9	Conclusion

The research stage 1 is initiated in phase 1 but implemented in phase 2. Stages 2 and 3 are implemented in phase 3 while the research findings, which are the outcome of phase 3, are addressed in phases 4 and 5 as illustrated in figure 5. Chapters 4 and 5 are not research phases but extensions of Chapter 3 where the rationale to measure awareness in SNs are justified, and the proactive approach is considered the best method of measurement.

Figure 5: Research stages implemented in phases (own compilation)



The research work commenced with a comprehensive review of the past related works (as presented in Chapter 3), where research questions were identified and placed in context. This was followed by the development of sOcialistOnline, a newly developed SN specifically

designed for this work. This is the second phase of this work and it is fully addressed in Chapter 6. Data-gathering and awareness measurement is the third phase, and it is presented in three different sub-phases namely: password cracker (observation/available information), quiz template (questionnaire), and intention-gathering. This phase forms the integral parts of this study and it is discussed comprehensively in Chapter 7. The result analysis is the fourth phase followed by the last phase – discussion and conclusion. These last two phases are treated in Chapters 8 and 9 respectively.

2.7 Summary

This chapter considered the concept of research paradigms together with their underlying philosophies, and provided a brief overview of available research designs and methodologies in SNs. The actual methodologies employed in this study were subsequently discussed in detail.

Owing to the fact that each of the two research methods has its individual strengths and weaknesses, this study used triangulation, which is an approach that combines both the quantitative (questionnaire) and the qualitative (observation/available data) methods of data collection. Another reason for using triangulation is that the postulated solution from this study integrates quantitative techniques (password cracking), whereas the data collection technique (available data) generates qualitative data. This combination technique was addressed for the author to get the best of each method and avoid their shortcomings towards implementing a non-incident statistics approach of measuring awareness.

Following the general overview of the research design, this chapter summarises the five phases of this study by looking at the objectives of each stage, how the study will be conducted and results be analysed, and the influence of findings from one phase on the design of the next. Phase one (past related works) will be discussed in Chapter 3, while phase two (sOcialistOnline) will be presented and implemented in Chapter 6. The results of the remaining phases will be presented in Chapter 8 to illustrate the use of a non-incident statistics approach towards measuring the awareness efforts.

However, to establish the originality of this work, this study had to conduct a comprehensive literature review on awareness limited to SN. This is what is addressed in detail in the next chapter.

CHAPTER 3 RELATED WORKS

3.1. Introduction

The awareness concept is not limited to teaching the users and giving lessons, but also considers human behaviour and changing people's attitudes. This is a difficult process which requires experimental research and measurement. An effective awareness programme is meant to start with the identification of the requirements and key problem areas, analysis of the root causes, and development of programmes that indicate corrective actions in SNs (Lacey 2009:5).

There is always scope for improving awareness in SNs no matter the type of the organisation or industry. According to Lacey (2009), expressing knowledge and awareness is relatively easy to fix, even if it requires consideration and planning; it is giving the right information to the right people in the right form. However, changing people's attitude is considered a much harder task; it involves a learning experience from an activity such as reading a book, watching a movie or partaking in a creative discussion. Changing the behaviour requires a clear understanding of the desired behaviour of the users, as well as acknowledgment of all the keystones of the enablers and blockers (Lacey 2009:34), as they relate to the SNs. Hence, lack of reliable metrics to measure the effectiveness of awareness and changes in behaviour is one of the factors that could contribute to an effective awareness programme.

The aim of this chapter is to provide an overview of the past related works. This chapter provides the theoretical foundation for these questions by addressing the following issues: theory or models applicable to awareness, privacy risks and security threats of SNs; techniques for securing SNs, and the effectiveness of awareness efforts. It emphasises the theories behind the measurement of effectiveness of awareness programmes to put some speculation regarding non-incident statistics approach to rest.

3.2 Background study

Almost every industry, including the banking and airline industries, have embraced the use of SNs. Southwest Airline, JetBlue Airways, Delta Airlines and Virgin America are using SNs such as Twitter, Facebook, YouTube and Flickr (Albert 2008:Internet). Among the services available on the Facebook profile of Virgin America are search flight, check flight status, fan

photos, customer review, videos/fan videos, and company information (Albert 2008:Internet). Southwest Airline, always the great innovator in real social communication, has been a big player in SNs since August 2011 (AirlineLeader 2011:Internet), and with over 1.785 million Twitter followers as at December 2014 (Socialbakers 2014:Internet). It focuses on using the Twitter channel to monitor and defuse potential mini-crises and to keep tabs on bigger issues. The airline chooses Twitter as its preferred SN based on its simplicity and ease of use.

Table 3 shows a comparison between Google+, Facebook and Twitter. MySpace, being the least secured against privacy threats among the top five SN (Judge 2011:5), is exempted from this table as media rarely compares it with SNs, other than Facebook. When compared with Facebook, a significant distinction lies on the level of customisation, and this is a major factor that lowers users' level of interest and distracts their attentions from MySpace (McNeil 2012:Internet). Unlike Facebook and Twitter, the MySpace layout comes with complex customization, which often confuses and frustrates users. Although not enforced, Facebook requests users to provide their true identity, a requirement that MySpace and Twitter do not have (Ciccone 2009:Internet; Prairienet 2011:Internet). Additionally, MySpace permits users to brighten their profiles using HTML and Cascading Style Sheets (CSS), whereas Facebook permits solely plain text (Jithin 2012:Internet; Sullivan 2007:5).

Table 3: Facebook vs Twitter vs Google+ (adapted from SocialCompare 2013:Internet)

Description	**Facebook**	**Twitter**	**Google+**
Website	Facebook.com	Twitter.com	Google.com
Lunch date	Feb 4, 2004	Mar 1, 2006	Feb 9, 2010
Last update	October 3, 2013	October 4, 2013	May 13, 2013
Chat	Y	Y	Y
Games	Y	N	N
Events management	Y	N	N
Support 3rd party app	Y	Y	N
Business profiles	Y	N	N
Verified accounts	N	Y	N

Description	Facebook	Twitter	Google+
Activity stream			
Friends updates	User gets update after a friend accepts his request. Then he receives the updates the friend wants to share with him	User gets updates directly from friends	User gets directly updates from friends he added into his circle
Excludes friends or groups from updates	Y	N	N
Post internet search results	N	Y	Y
Questions and polls	Y	N	N
Adding location to posts	Y	N	Y
Video calling			
Video group calling	N	N	Y
Private group chats	N	N	Y
Public group chats	N	N	Y
Watch YouTube video	Y	N	Y
Supported OS and browsers	Windows, MAC Chrome, Firefox, IE, Safari		Windows, Mac, Chrome OS, Ubuntu, IE, Debian based linux distributions; Chrome, Firefox, Safari.

According to a study conducted by Barracuda Networks Inc., between September and October 2011, Facebook appeared to be the SN being used most with 92.9% usage, followed by LinkedIn (75.6%), Twitter (74.8%), Google+ (55.5%), and Myspace (5.9%) (Judge 2011:5). The total percentage utilization is higher than 100 because SN users are not confined to only one SN; a typical user makes use of two or more SNs such as Facebook and Twitter. LinkedIn are the most business-friendly by being the network least blocked or limited by businesses, followed by Google+, Twitter, Facebook and MySpace, respectively (Judge 2011:5). The same study also reported LinkedIn as the safest SN with Facebook and MySpace being the least secured against privacy threats. Accordingly and until 2012 when LinkedIn was hacked, users were more content with its privacy controls, but displeased with Facebook (Judge 2011:15). These safety reasons that score LinkedIn high in items 2, 3 and 4 in table 4 call for a serious review of privacy risks and security threats of SNs.

Table 4: Comparison between some popular SNs (own compilation)

S/N	Description	Facebook	LinkedIn	Twitter	Google+	MySpace
1	% rate of usage	92.9	75.6	74.8	55.5	5.9
2	% of least blocked by workplaces	31.0	20.0	25.0	24.0	34.0
3	% of users feeling unsafe	40.0	14.0	28.0	21.0	84.0
4	% of users displeased with privacy controls	51.0	25.0	30.0	29.0	65.0

3.3. An overview of information systems and security theories

Organisations generally make use of technology to protect their data and information. However, they also depend on their employees and the technology users to achieve this security objective. Therefore, since SN users assume certain roles and are also responsible for protecting their resources on the network, this research is interested in those theories (as introduced in section 2.4) and factors that drive individuals to perform their roles and meet their responsibilities. This section will therefore examine the existing theories and models in the field of information system (IS) and information security especially as it relates to knowledge and attitude of KAB.

3.3.1 Theory of reasoned action (TRA)

The theory of reasoned action (TRA) originated from social psychology and it is regarded as the famous theory of human behaviour. It proposes that "a person's performance of a specified behaviour is determined by his or her behavioural intention, which is jointly determined by the person's attitude and subjective norm" (Davis 1989:983). Behavioural intention refers to a gauge of the strength of an individual's intent to perform specified (security) behaviour. Generally, subjective norm refers to someone's perception that most people who are important to him think he should or should not perform the behaviour in question while attitude is defined as "a person's positive or negative feelings about executing the requisite secured behaviour" (Padayachee 2013:66).

The most important part of TRA from IS's perception is its assertion that other factors can only influence behaviour indirectly by virtue of the influence it brings to bear on attitude, subjective

norm or their relative weights. "Other factors" here are variables such as "system design, user characteristics, task characteristics, nature of the development or implementation process, political influences, and organisational structure (Davis, 1989:984).

3.3.2 Rational choice theory (RTC)

Rational Choice Theory (RCT) is an economic approach that theoretically explains the way people take decisions when faced with choices (Bulgurcu 2010:527). RCT maintains that "an individual determines how he will act by balancing the costs and benefits of his options. For its economical and elegant explanation, the theory has been widely applied to the study of individual, social, and economic behaviours in many contexts" (McCarthy 2002). For instance, Becker (1968) embraced the RCT perspective in his economic approach to crime and argued that "a criminal maximizes his expected benefits from an illicit activity in excess of the expected cost of punishment".

In making a rational decision, an individual will first identify the alternative courses of action (Paternoster and Pogarsky 2009) before contemplating on the probable outcomes of each of the courses. Ordinarily, outcomes are products of action taken, and various outcomes may arise from just one action. However, "since people have preferences for outcomes, each outcome can be perceived to be associated with a cost or a benefit depending on how much satisfaction the outcome will give to the individual. Hence, overall assessment of individual costs-benefits from a course of action depends on the individual's perception of potential outcomes associated with that course of action" (McCarthy 2002). Therefore, the individual weighs his overall assessments of costs and benefits of courses of action to determine the best alternative.

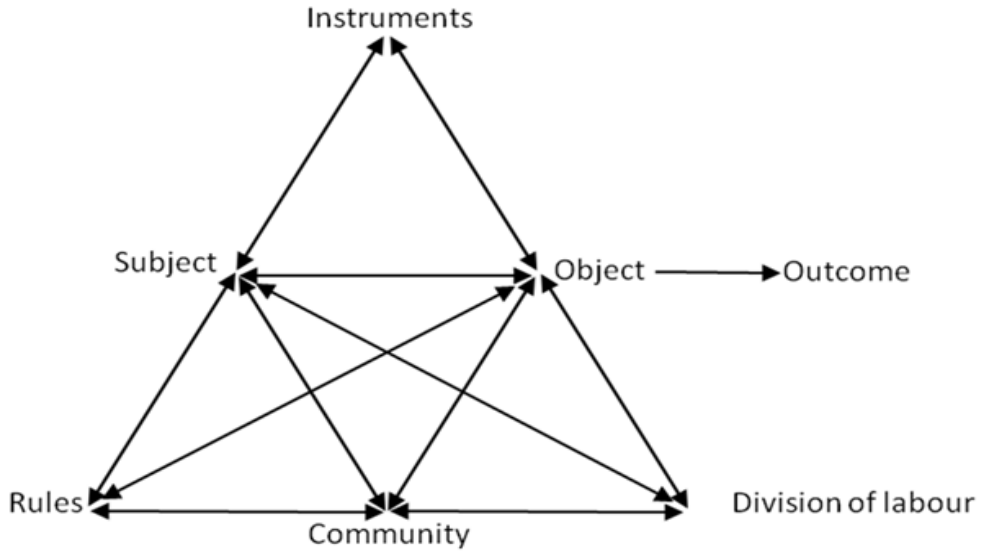
3.3.3 Activity theory (AT)

According to Kaptelinin (2013:4), "the fundamental concept of activity theory (AT) is the emphasis on activity which focuses on the interaction between the subjects and the objects". The main focus of AT, which remains its key character, is the opinionated researches into the relationship between the individuals and their mediated tools or technology (Hashim and Jones 2007). Activities is of more importance in AT, as they (activities) work towards achieving the goals and objectives of any research.

The AT is applicable in various disciplines including management, culture, education, psychology, IS, and information security, which are all linked to human interactions (Hashim and Jones 2007). It particularly applies human activities to investigate research findings that

are divided into tools, object and subject (Hyland 1998). "Where 'subject' refers to the participants involved in the research, the 'object' refers to the activities carried out by the participants, and the 'tool' is the mediating device by which the action is executed" (Hyland 1998). Engeström (2001) altered the AT to produce a new version that includes 'rules' which "determine how and why individuals may act and are as a result of conditioning" (Hyland 1998; Verenikina 2001). The new version also includes both the 'community' where "groups of activities and teams of workers/users are anchored and can be analysed," and the 'division of labour' in which "activities are broken into smaller units to be undertaken by the participants making up the community" (Hyland 1998; Verenikina 2001). These perceptions are as described in Figure 6 and help to focus on the relationship between the subjects and the objects of this study as identified in section 2.4.

Figure 6: Engetrom's activity theory model (adapted from Engetrom 1987:77)



3.3.4 KAB model

Most awareness solutions are built around the KAB model, which is centred principally on human knowledge (Kruger & Kearney 2005:3). The model postulates that knowledge accumulation in a particular behaviour (IS, health, environment, education, etc.) instigates a change in attitude. The model principally substantiates the influence of knowledge on people's behaviour, which in turn enforces changes in attitude and behaviour (Khan, et al. 2011:10863).

3.3.5 System-determined, interaction-determined and people-determined theories

The customised referent theories for this work are system-determined, interaction-determined and people-determined, which are Markus's three theories as presented by Myers and Avison

(2002). Since "the basic assumptions underlying the theories can be examined and compared with facts in the real world" (Myers & Avison 2002:22), the assumptions underlying information security and system utilization are *adapted* from Markus's competing theories of system and people's resistance to study the impacts of awareness in SN. The concepts, from dissimilar models namely AT, KAB, TRA, TPB and RTC are practically related to the global construct or theme comprising dependent and independent variables (section 2.3.1; figure 2) namely awareness measurement: *How to measure*, *What to measure*, *Measurement approaches*, *Problems in measurement*, *Security techniques*, *Awareness benchmarking* and *Metrics, privacy risk and security threats*. The conceptual relationships between these concepts are discussed in sections 2.3.2 and 3.3, and the theories are detailed as follows:

3.3.5.1 System-determined theory

In the *system-determined theory*, resistance or non-utilization is attributed to intrinsic features of the implemented system. Explanations in line with this theory are that people oppose systems with technical deficiencies, systems with poor ergonomic design, and systems that lack user friendliness. The system-determined theory predicts that acceptance or resistance of a given system in any organization is attributable to its design features including security settings. The underlying assumption of the system-determined theory is that non utilization is an attribute of system users (Myers & Avison 2002:32).

3.3.5.2 Interaction theory

The *interaction theory* attributes resistance or non-utilization of systems based on an interaction between people characteristics and system characteristics. An explanation drawn from the interaction theory is resistance arising from interaction of the system's technical design features with the social milieu in which the system is used. The underlying assumption for the interaction theory is that non-utilization or insecure behaviour is a result of the privacy setting, system users and system designers. The interaction theory can explain dissimilar outcomes for system implementations in diverse settings, as well as the dissimilar reactions by the same user group in diverse settings (Myers & Avison 2002:47).

3.3.5.3 People-determined theory

The *people-determined theory* includes inherent people characteristics, for example, cognitive style, personality traits, and human nature. The people-determined theory assumes that resistance is a characteristic of the system user (Myers & Avison 2002:49) and that peoples'

resistance to IS is a function of those factors internal to the person or the group (Myers 2013:76). The theory is good at predicting the rejection of all systems in a setting in which any one system is resisted (Myers & Avison 2002:22).

3.4. Privacy risks and security threats of SNs

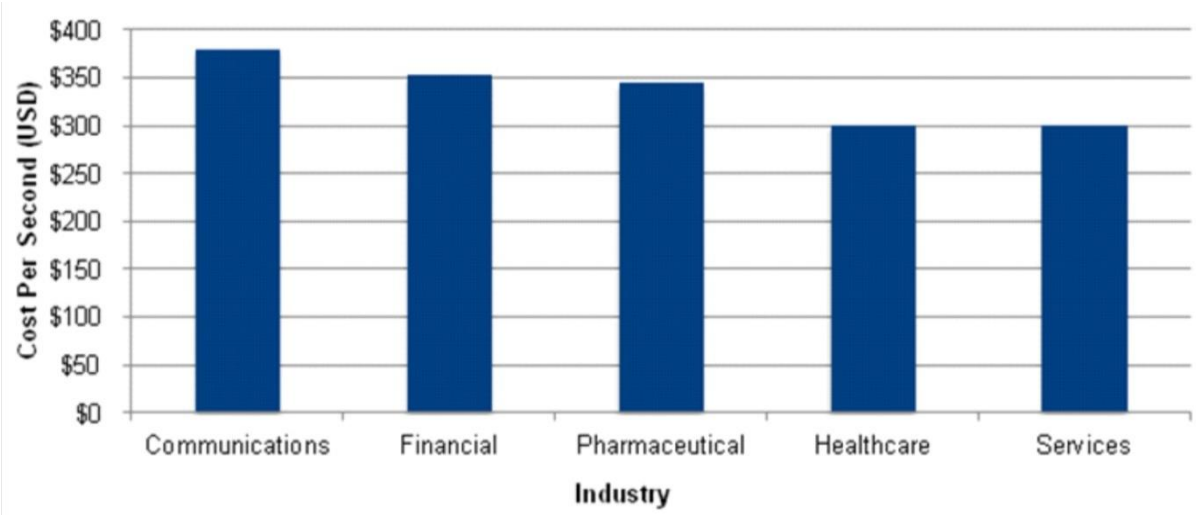
While several literature sources emphasise the importance of awareness in SNs (Brodie 2009:9-20; ENISA 2007:3-7; Hinson 2012:Internet; PriceWaterHouseCoopers 2010:Internet), Samuel and Samson (2012:17) surprisingly argue that security education may yield negative results against the expectation and thereby promote the potential risks that users are exposing themselves to. They report that if users are well informed about the risk in disclosing credit card details via emails, but the attack approach is changed to be launched through telephone requests, then such users could be at risk for simply following what they were told to do.

Many websites have been built by public interest groups reporting the privacy threats of SNs as well as the possible preventive measures. These groups include the International Working Party on Data Protection in Telecommunications (IWGDPT), the Canadian Internet Policy and Public Interest Clinic (CIPPIC), and the Electronic Privacy Information Centre (EPIC). The EPIC website and CIPPIC's complaints with the Canadian Privacy Commissioner specifically give a better description of these privacy threats but fail to offer a general recommendation to the policymakers (Riphagen 2008:12). Similarly, IWPDPT's report and ENISA's position paper introduce some privacy preventive measures for SN users, but they are silent about the methodology required to identify and prioritise the risks (Riphagen 2008:13). Meanwhile, experts never agree on which privacy risks will be given immediate preventive attention and as a result, cyber-attacks continue to grow (Smith 2012:Internet).

3.4.1 Cyber-attacks

As at 2012, cyber-attacks remain the second greatest threat in Britain, after terrorism (Smith 2012:Internet). This ranking comes as no surprise as cyber-attacks result in the loss of millions of dollars, sometimes without the company's knowledge. In 2010, Kroll Cyber-Security presented figure 7 to exhibit the industries with the highest per-second cost of inadequate cyber-security protection. The communication industry appears to be the most vulnerable going by the bar chart. Generally speaking, SNs are web applications and can also be vulnerable to the same cyber-attack.

Figure 7: Cost of cyber-security attacks by industry (adapted from Smith 2012:Internet)



Similarly in a 2010 Symantec survey of small- and mid-sized businesses (SMB), companies including some SNs reported the areas in which they experienced the biggest losses (Smith 2012:Internet), as represented in figure 8. Lost productivity (which is business continuity in SNs) was the highest, followed by revenue loss.

Figure 8: Losses incurred from cyber-attacks (adapted from Smith 2012:Internet)

Following this in November 2010, both a French research company and the Polytechnic Institute of New York University notified Skype (a web application and an internet industry) about a flaw that allows hackers to track down users, based on their IP addresses (Smith 2012:Internet). Unfortunately as at December 2012, the same institutions retested the flaw and found that Skype had still not resolved this problem. Since Skype reported that 37% of their

663 million users use their technology for business and social purposes, this flaw presents a cyber-security risk for companies and SNs as well.

3.4.2 Safeguarding users' identity

Surprisingly, SNs are still not very sensitive to the issue of IS. At a technology conference organised in January 2010, the Chief Executive Officer (CEO) of Facebook, Mark Zuckerberg stated that "privacy is no longer a social norm as users have adapted to sharing information online over blogs and other social media and, in turn, the company has structured its privacy settings accordingly" (ReutersSummits 2010:Internet). Exactly six months thereafter (July 2010), a program was created by a hacker that extracted and publicised sensitive private data of over 100 million Facebook users that did not reset their privacy settings to hide their profile pages from search engines (HelpNetSecurity 2010:Internet).

Before Google Buzz was released in February 2010, Google was charged with a class-action lawsuit in a California federal court and also at the Federal Trade Commission (FTC). Google was accused of mechanically activating and publicly generating accessible lists of followers collected from users' Gtalk conversations and Gmail accounts (PCWorld 2010:Internet). In June 2010, Twitter, submitted to the U.S.A. FTC charges that it deceived customers and endangered their privacy by failing to safeguard their private data (FTC 2010:Internet). This validates the position of Gross, Acquisti, and Heinz (2005:12), that risks associated with SNs are not limited to identity theft, online and physical stalking, but also range from embarrassment to price discrimination and blackmailing. Subsequently, awareness techniques for securing SNs are absolutely required to mitigate the risks.

The general and continuous growth in Web 2.0 applications and the associated economic value of SNs, in particular, have come with new security challenges which security and privacy advocates are yet to adequately address (Heidari 2010:3). Privacy risks such as blackmailing, personal embarrassment, online or physical stalking differ amongst people, and rely much upon a particular context. When looking at SNs exploitation, the overriding strategy for sensitive private data collection right from the beginning necessitates the need to re-evaluate traditional privacy approaches that are primarily meant to safeguard a user's identity in the past (Weiss 2007:8). It is, therefore, necessary for the new privacy approaches to concentrate on safeguarding fundamentals, which can be set by individual. Such prerequisites should be self-controlled and support protection mechanisms for effective data management and administration.

3.5. Techniques for securing SNs

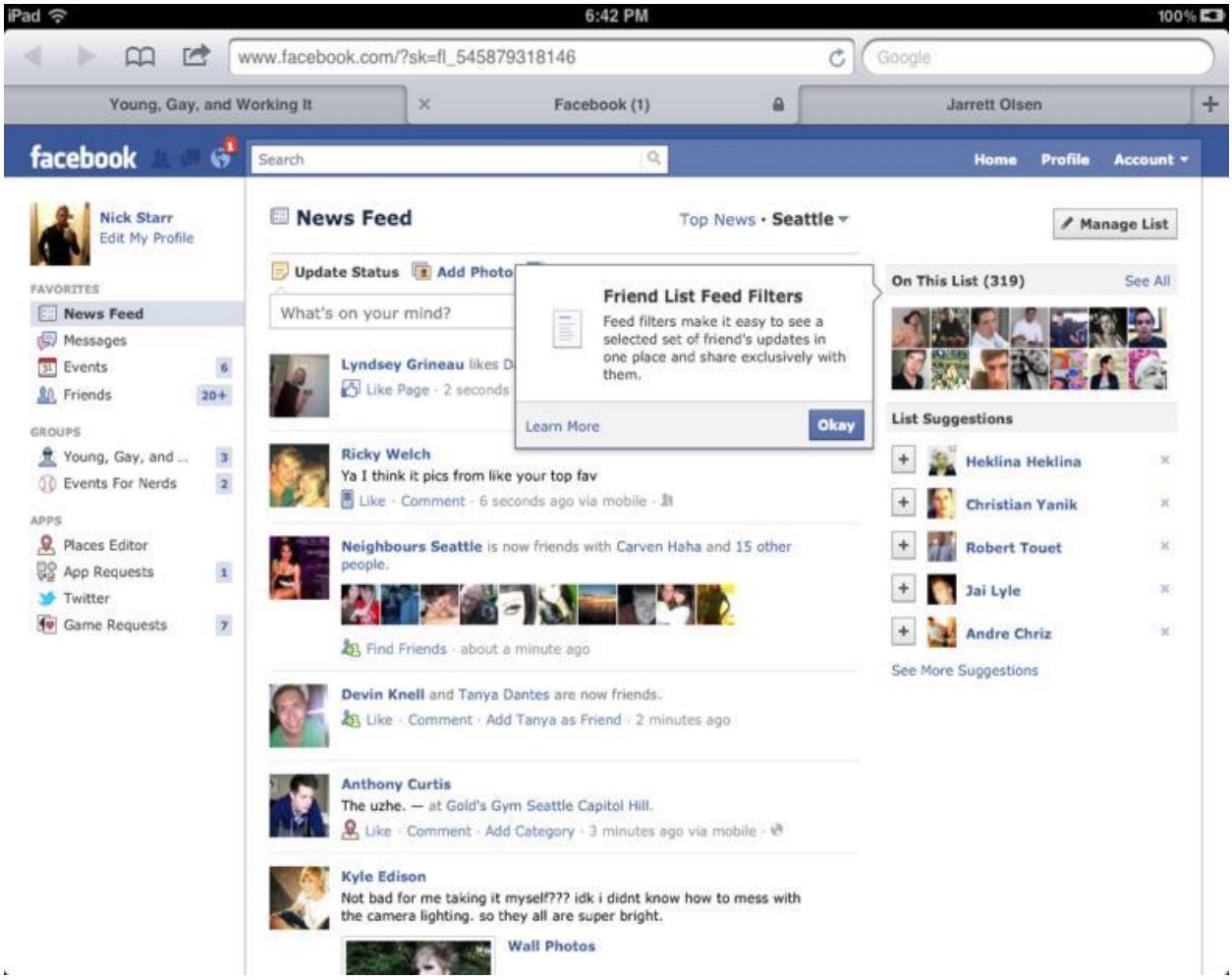
The issue of information security on SNs is major, but has always been addressed by the SNs in favour of emphasising user growth and brand marketing. Several techniques are now established to build security into the SNs, with the main emphasis on data privacy as fundamental rights of every user. Some of these techniques are technical or awareness related in nature, and include customisation of access controls, effective private settings, privacy lens, password monitoring and standardisation, privacy awareness and customisation. These techniques are employed to secure sOcialistOnline for this research purpose, and details are presented in Chapter 6.

Giles (2007:17-24) highlighted some security design patterns and measures that can be used and practiced by service providers to prevent possible ways that attackers may use to attack users' information. He categorises security measures as government policy, provider and corporate policy, technical recommendations, research and standardisation. However, to remain within the scope of this study, this author classifies the security techniques as technical controls and awareness controls. The techniques generally make use of privacy enhancing technology (PET) and are considered to address the principles of data minimisation and data sovereignty (section 6.6).

3.5.1 Technical controls

Facebook has many times initiated architectural features that exposed data, thereby making SN users uncomfortable (Lucas & Borisov 2008:2). The introduction of a news feed (figure 9) is a noted example in which the activities of one's friends are amassed into one page. In this case, an individual who ordinarily is not included in the "audience of the post" of another user can see such a user's comment (Facebook 2013:Internet). This is, therefore, a confirmation that privacy breaches are still possible, whether or not users painstakingly configure their privacy settings, especially now that privacy controls do not have much impact on how Facebook handles its back-end data, but only limit information flow within the Facebook interface.

Figure 9: A news feed (adapted from Parr 2011:Internet)



This risk was minimised by Lucas and Borisov (2008), who made use of encryption technology to introduce a design capable of safeguarding all data coming out of Facebook. Their architectural design swaps security for usability in order to minimise the disturbance on a user's workflow, and at the same time retaining universal accessibility. Although this was not implemented by Facebook, the researchers came up with a prototype Facebook application that makes use of proxy cryptography to resolve major restrictions on the Facebook platform.

In spite of vendors' calls necessitating the importance of security products, many critical security activities have not and cannot be automated (Stephanou & Dagada 2008:3). This is because only a small percentage of information security is maintained by technical security measures, while its greater percentage depends on the user (Mataracioglu & Ozkan 2010:4). Organisations have invested heavily in firewalls, antivirus systems and other technologies, yet they are still suffering from severe information security breaches and the problems are getting worse (Gartner 2011:Internet).

Technologies that offer security still have to be effectively run by people, implying that organisations cannot achieve its security desire without people. However, since the individual is generally considered as the weakest link in the information security circle (Van Niekerk & Von Solms 2004:2), it is clearly required that users are given proper training on information security policies. The objective is to have effective policy implementation by ensuring that only the required policies are employed and that the policies are not misunderstood by users.

3.5.2 Awareness techniques in SNs

Much research has been done on awareness techniques but most of it is not based on a theoretical model, instead, they only guide against the right methods to use (Stephanou & Dagada 2008:6). For example, the research done by Heidari (2010), Hinson (2012), and Wolf (2010) all show detailed work on the methods to use. Most of these methods are elaborated on in Chapter 6.

Kumaraguru, Rhee, Acquisti, Cranor, Hong and Nunge's research (2007) proved that awareness materials can be effective when used. However, as users tend to recognise phishing sites better, the online materials that tend to create users' awareness on phishing threats are becoming more effective. They also advocate for an improved quality of awareness materials, as well as better awareness techniques to enhance user understanding of the same materials.

Johnson (2012:8), in his doctoral research conducted at the University of Lagos in May 2012, argues that too much is expected from the audience undermining the position that security processes can only be effective when the audience have a good security support and appreciate security requirements. On this basis and by applying background training, Jagatic, Johnson, Jakobsson, and Menczer (2007:96) were able to prove that it is very easy (through SNs in particular) to capture a huge amount of data for effective phishing attacks. They also attempted, but with no success, to measure the influence of social context information on phishing attacks. What makes their work different was that emails were spoofed to deceive users as if they were from friends in the SN, and in the end the total number of victims to this phishing attack is higher than expected (Jagatic et al. 2007:97).

Sommers and Robinson (2004:379) demonstrated the possible use of quiz and awareness videos to train students at the Virginia Commonwealth University, U.S.A. However, the researchers acknowledged that they did not have the means to measure the resultant impacts (Stephanou & Dagada 2008:6). They only showed a video clip for respondents to take a quiz afterwards. The security awareness campaign was deployed by McCoy and Fowler (2004:349)

at another American university campus. However, they too failed to apply any metrics and, therefore, found it very difficult to achieve.

ENISA identified a wide range of awareness techniques. However, in their research conducted in 2007, classroom training was considered the most effective while promotional materials, such as pens, were considered least effective (ENISA 2007:8-13).

3.6. Effectiveness of awareness initiatives

Many experts agree that awareness is effective, while others disagree, claiming that awareness is ineffective (Veseli 2011:11). For example, Hassan and Hussin (2010) criticise the effectiveness of awareness, arguing that awareness has been promoted for many years as being fundamental to information security practice. Their statements unveil that very few research studies have been done regarding the effectiveness and efficiency of awareness.

Research has been exhausted in the realm of awareness, but literature still lacks proof of the effectiveness of awareness methods from psychological theories and they are still silent on the fundamental assumptions of these methods. However, in their own study concluded in March 2011, Khan, Alghathbar, Nabi and Khan (2011) evaluated the effectiveness of different awareness tools and techniques on the basis of psychological models and theories. They succeeded in describing the processes needed to measure awareness in an organisation.

The importance of awareness is also discussed by many researchers and organisations, but very few empirical studies are done, and none of them offer a technique that is effective in behavioural change (Veseli 2011:11). Similarly, very few experiments are done in measuring the effectiveness of the changes in human behaviour (attitude), amongst which are Carnegie Mellon University (Spice 2007:Internet), CISO (a large financial service) German organisation (Williams 2007), and the United States Military Academy.

3.7. Measurement of the effectiveness of awareness programmes

Although recent studies have already looked into the effectiveness of awareness efforts, they have always been focusing on phishing threats that are known for showing the effectiveness of classroom-based training, email-based training and web-based awareness material. Examining behavioural aspects and measurement of the effectiveness of overall awareness have been mostly neglected (Stephanou & Dagada 2008:8). For instance, in the research conducted by Albrechtsen and Hovden (2010) and Wolf (2010), the effectiveness of security awareness was examined with particular interest in phishing threats.

3.7.1 Behavioural measurement

Previous research have invariably emphasised the importance of getting people to act correctly. However, since 2004, there have been further specific concentrations on behavioural aspects of security. For example, many studies on behavioural information security have demonstrated the relationship between employee job attitude and information security behaviours (Stanton, Stam, Guzman & Caldera 2003); the classes of information security behaviours that are in existence (Stanton, Stam, Mastrangelo & Jolton, 2005); the controlling factors of information security behaviours (Leach, 2003) and the significance of attitudes and intentions towards the rationale behind some employees not complying with information security policies (Pahnila, Siponen & Mahmood 2007).

Similarly, Stanton et al. (2005:124,131) applied a simple correlation to research the consequences of good password practices (such as strong-password selection), as perceived by workers, on training and awareness, skills of monitoring workers, as well as on the organisational edges. These practices are often referred to as naive end-user security behaviours. These attitudinal behaviours are common to people of neutral intention and low expertise. They concluded that the association between password-sharing behaviour and training, awareness, organisational rewards and knowledge of being monitored cannot be substantiated.

In the same way, Vroom and Von Solms (2004:191-192,194, 197) appreciated the relevance of users' behaviour in the security circle but only from an auditing point of view. Their argument was that even though auditors may express their independent opinion on an organisation's arrangement, unlike quantitative approaches, employee behaviour is never measured because of the difficulties involved, and its vulnerability to errors.

3.7.2 Quantitative and qualitative approaches

A wide range of completely different strategies is being adopted to measure awareness efforts, however, organisations do not seem to find it easy to implement effective quantitative metrics (ENISA 2007:2). Each organisation adopts different methods, both quantitative and qualitative approaches, to measure the effectiveness of their awareness activities. Nyabando (2008:101) agrees that more extensive qualitative and quantitative studies are needed to understand the disparities between awareness and practice.

In 2005, a prototype model was developed by Kruger and Kearney (2005) to measure awareness effectiveness in an international gold-mining company, based on knowledge, attitude and behaviour – KAB (refer to in section 5.6.1). However, their work failed to study the basic theory

behind the model. Similarly, Hagen, Albrechtsen and Hovden (2008) analysed responses to research questions from 87 information security managers in Norwegian organisations. Furthermore, in a research study concluded in September 2010, Albrechtsen and Hovden (2010) identified IS-related discussions as a tool effective enough to raise user awareness, although comparatively their study approach is judged to be less effective.

Wolf (2010:9) reported that there were some unconventional methods used to study and measure users' awareness. One of the notable methods was employed by Dodge, Carver and Ferguson (2007:73-80), who used phishing emails to detect users that clicked on potentially malicious links in emails. Briggs (2009), who described how software was implemented to examine network traffic for Personally Identifiable Information (PII) that was being transmitted unencrypted over a campus network, made another attempt. Meister and Biermann (2008:343-350), using similar methods, detailed the use of a worm that was created to test the users' ability to detect phishing attempts in their research. Nagy and Pecho (2009:321-325) tested Facebook users' ability to detect and measure phishing attacks by attempting to friend as many unknown people as possible.

3.7.3 Incident statistic approach

The recent report of ABC (2013) submitted in November 2012 classified all these methods as incident statistics approaches to measure awareness. They are adjudged to be incident statistics, since the measurement of their effectiveness is based on the occurrence of an event or success of an attack.

Research conducted by ENISA (2007:17) highlighted 12 different metrics as effective in measuring the success of awareness activities, all of which are driven by incident statistics. The most popular overall is the measure of internal protection, where policy breaches from audit reports are being used as a measure. This is followed by the effectiveness and efficiency measure, where the experience of the respondents on security incidents counts extensively. The common metrics include the quantity of incidents resulting from insecure human deeds and a root cause analysis of the most terrible incidents (section 5.7.3).

Even though the statistics generated from this method are often of great interest to senior management, ENISA submitted that the approach may not be the most effective because it may not necessarily give a true reflection of awareness. They admit that awareness is not the sole determinant factor of the occurrence of incidents, but also the extent of the occurrence of

attacks (ENISA 2007:16). Ultimately, the trend of attack may better indicate SA, but in practice, people will always base their action on individual trends.

Surveys and questionnaires are adjudged to be the most popular measurement instrument as evident by the large number of studies that used them, among which are Bulgurcu, Cavusoglu, and Benbasat (2009:476-481); Chan and Wei (2009:68-71); Kolb and Abdullah (2009:103-107) and Marks and Rezgui (2009:1-7). Marks and Rezgui (2009) are the only researchers who use researcher observation as part of the measurement. They use a combination of surveys, interviews, case studies and observations to form their analysis (Wolf 2010:10).

3.8 Summary

In this chapter, a comprehensive literature review on cyber-security awareness is done to ensure that related approaches of measuring effectiveness of awareness on SNs have not been identified or implemented. Towards achieving this target, the following research sub-questions, raised in section 1.4, were addressed: Which metrics can be applied to measure online user behaviour in SNs? Which controls are available to measure awareness? Why should technical control be explored as an option to measure awareness in SNs? The primary research question and the remaining sub-questions will be addressed later in the study.

Following the theoretical review of models applicable to awareness, this chapter employed the works of Stanton et al. (2005:124,131) and Vroom and Von Solms (2004:191-192,194,197) to address research question 1.3.2.1. Vroom and Von Solms (2004) succeeded in classifying auditing as a control measure of human behaviour, however, many researchers have principally censured their findings on the premise that employee behaviour does not seem to be measured, and that there are several factors that could hinder the process of auditing the employee. In this context the privacy risks of SNs and their security threats were reviewed to support the argument that the growing economic value of SNs has indeed introduced several security and privacy issues.

The emphasis laid on the importance of awareness in SNs by several literature sources (Brodie 2009:9-20; ENISA 2007:3-7; Hinson 2012:Internet; PriceWaterHouseCoopers 2010:Internet), and the latest work of Esma et al. (2010) and Asim et al. (2010) confirm that some of these risks have already been addressed by researchers. However, authors are yet to carry out a detailed investigation to determine the most effective technique of measuring awareness programme in SNs. Although, Johnson (2012) attempted to address this challenge by only

examining the relationship of awareness training components, his study left the general awareness techniques unattended to.

Therefore, in the next chapter this study comprehensively considers various awareness techniques that must be recognized for their effectiveness to be possibly measured – an act that stands as the primary aim of this study.

CHAPTER 4 RATIONALES FOR AWARENESS IN SNs

4.1. Introduction

This chapter focuses on the justification for awareness in SNs by addressing the need for adequate data protection, and investigating the motivation behind the emphasis on awareness techniques. Available awareness raising techniques will be examined to appreciate the potential impacts of awareness programmes in securing SNs.

Well-established management security standards like the SABS ISO/IEC 27000, ISO/IEC 27001 and the Organisation for Economic Co-operation and Development's (OECD) guidelines for IS security have been promoting the importance of awareness issues to people. According to the Computer Security Institute (CSI) 2006 survey report, the average individual in an organisation thought that their organisations were under awareness investigation. Their 2007 report (CSI 2007) also indicated a significant rise in the importance of awareness perceived. Similarly, the Republic of South Africa Ministry of Justice and Constitutional Development (MJCD) passed the Protection of Personal Information (POPI) Bill, which highlights eight information protection principles (POPI 2009:10-16) including awareness. This Bill became an Act in late 2013. All these results are good indications that organisations are beginning to realise the importance of awareness.

However, in line with submissions of Hinson (2012:Internet) and Johnson (2012:5), inadequate user awareness remains the single most important thing every SN owner should tackle. This explains why most often there are security programs that have excellent technical components, but no significant improvement in security behaviour due to the way technology is being used. Security experts have all accepted that regardless of the technology in place for data protection, people still represent the biggest problem. An appropriate awareness technique is, therefore, required to create adequate awareness to users of SNs.

4.2. Background

Some SNs already devote a lot of time and effort establishing technical controls to protect information but leaving the final user unaware of security topics, an act that is capable of slowing down technology investments and advancements. It is often forgotten that computers and technology are mere tools, and that it is the human being that is operating and abusing these tools. While many technical means are used to secure SNs, the individual user remains the last line – and frequently the weakest link – in the network defence (Boss 2007:27). With the

growth of SNs, it is becoming harder to monitor and protect SN users and their activity effectively because the tasks of security programmers become increasingly spread out (Collins 2010:Internet).

In an attempt to put potential threats under control, the major SN now empowers their users to be in control of their privacy settings to restrict unauthorised access to their information. However, privacy settings may still not ensure absolute privacy if the existing vulnerabilities in Facebook are taken into account (Geary 2011: Internet). By means of a loophole discovered on Facebook in 2012 for instance, users can reactivate and deactivate their accounts at will, but the privacy settings for any deactivated account cannot be amended (Potalinski 2012:Internet). This flaw is dangerous and calls for immediate attention.

The implication of the above is straightforward. Where a friend request is already accepted by a friend to view a Facebook user profile's contents and, perhaps, such a friend now deactivates his/her own account for whatever reason, such a Facebook user cannot limit his privacy settings already linked with the account of that friend pending when the friend reactivates his account. Even when he/she is ready to reactivate his/her account, the Facebook user will have to be online simultaneously with the friend to be able to change back his privacy settings (Potalinski 2012:Internet). The alternative way is for such a user to apply a universal change to all his/her friends. The main challenge with this concept of SNs privacy, and which calls for awareness techniques, is the dichotomy between public and private spheres. This is termed the secrecy paradigm, and was addressed by Solove (2006), who stated that privacy is a concept in disarray.

The secrecy paradigm

This is a rule or directive proposed to detect privacy threats using users' personal information. Here, privacy is seen as an absolute secrecy, where privacy violation is possible only when concealed information is divulged. This implies that unconcealed information does not confer any privacy interest (Solove 2006:497). Hence, the privacy paradigm concludes that information already opened to general public can no longer be private and can, therefore, be used without privacy threats (Solove 2006:537).

The focus of the secrecy paradigm is on unwanted publicity, breached confidentiality, and reputational damages. These threats do not pose a major challenge to databases because these complications do not arise when identity-relevant information is used to focus on privacy threats. Public information, like names and photographs displayed on the internet forum can be used in combination to cause threats or damages. The secrecy paradigm does not recognise threats here, while the focus on identity-relevant information and potential threats does

(Riphagen 2008:25). Strahilevitz (2005) postulates an SN privacy theory to address challenges of the secrecy paradigm as to data classification into private or public. However, his theory did not achieve much as it only succeeded in determining when a secret turns out to be open and thereby undermines privacy (Riphagen 2008:41).

4.3. Reasons for data protection on SNs

Van den Hoven and Manders-Huits (2006:2) provide a good overview of reasons why access to this information should be constrained. Their moral analysis uniquely covers a broad range analysis on moral issues as it relates to identity and safety, but with the focal point on identity itself and reasons for being valuable to human beings. Most of their claims could not be legally substantiated because it is both difficult to ascertain the existence of threats, and to measure it monetarily (Riphagen 2008:26). They specifically outlined the following reasons as the major reasons why data protection on SNs is a must:

1. Information-based threats.
2. Informational inequality.
3. Purpose specification and use limitation.
4. Least-authority principle.
5. Restriction on moral autonomy.

These reasons are discussed in the following sub-sections.

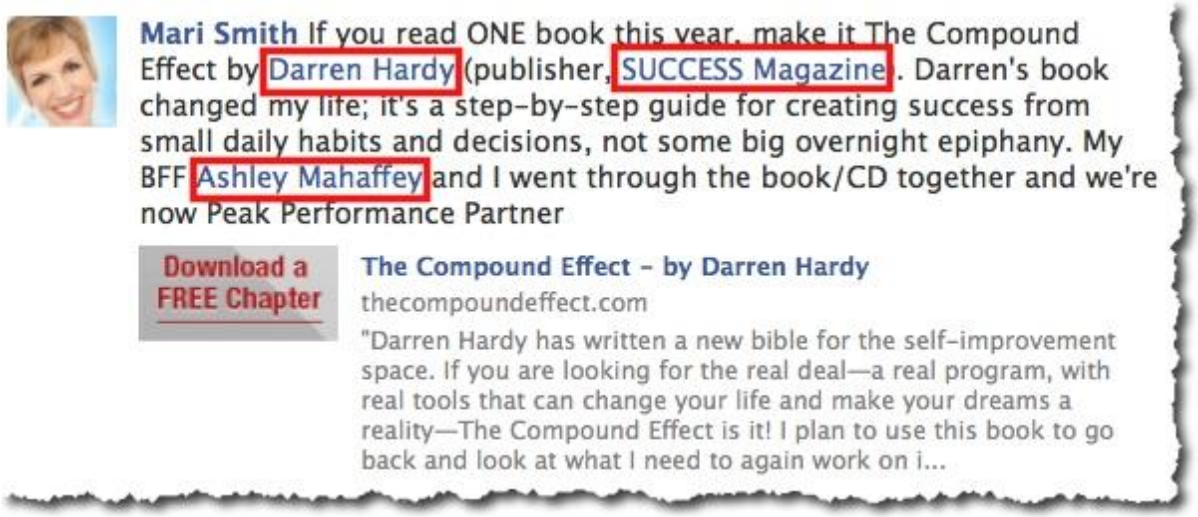
4.3.1. Information-based threats

Information-based threats are threats from crimes that are committed as a result of the adequate collection of information on the subject, and they form a major reason for the need for adequate data protection. A typical example is the gathering of snippets of identity-relevant data at different occasions that could be used in combination to deceitfully recapture someone's photographs with first and last names mentioned. Another good example is identity theft where an extensive knowledge of certain information about the subject is required before an attack can be launched. For instance, bank account numbers of a target are required before a fraudulent credit can be obtained from his account, and an employee's work hours are needed to establish the best time to attack his house.

This is a common practice amongst SNs, being referred to as tagging and gespot on Facebook and Dutch platforms respectively (Riphagen 2008:27). Someone else's picture can be uploaded and tagged with either his name or the name of another person. Users may also opt to tag or untag themselves, and even choose to be alerted when they are tagged. A typical example is presented in figure 10 and figure 11 where snippets of text are tagged to a person's profile/picture by a third party and eventually divulged to his potential employer when the former conducted a background check on him. The availability coupled with the ease of obtaining users' profiles is making SNs more vulnerable to various attacks.

Figure 10: Tagging on Facebook (adapted from Smith 2011:Internet)

Figure 11: Tagging on Facebook (adapted from Smith 2011:Internet)



To the best of the author's knowledge, no conventional laws and regulations have been able to address these issues to date. As at May 2008, the above challenges were attempted to be addressed by only two American tort laws – the private facts tort and the appropriation tort.

Even at that, the two torts could not easily measure the possible monetary damages, and also find it difficult to argue that data already posted on an SN are still private. Riphagen (2008:12) came up with an approach whereby harmful activities are arranged in groups of data collection, processing or dissemination, and threat is defined by reasons behind securing access to identity-related data highlighted in section 4.3.

4.3.2. Informational inequality

There exists a market for identity data where information relating to purchases and preferences are gathered (by organisations) to create customers' profiles, mainly for marketing and price discrimination. However, care must be taken to ensure that only complete and genuine data are collected (POPI 2009:13), and the responsible party must not lose focus of the objectives behind the exercise. This is called information quality, the fifth principle of information protection (POPI 2009:3).

Generally, most people are not fully aware of the market for their private data. Hence, they are unable to negotiate (or understand) what is offered in place of their identity-related information. This is referred to as information inequality, and it naturally describes the inability of SNs users to dictate the usage of their information on their profiles.

Although Europe has come up with regulations concerning secondary use, it is not properly enforced and users can still not negotiate with SNs about the use of their data (Riphagen 2008:27). Ordinarily, users are not under any obligation to complete every field of information on SNs; users easily get inspired by the design and construction of SNs to upload as much information as possible. In addition, the services offered by SNs are somehow difficult to unbundle, because it is presently impossible for users to know the size of the audience accessing their contents (ENISA 2007:3). A serious threat should, therefore, be envisaged if identity-relevant information eventually gets into the wrong hands.

Referring to the tagged photo at the party, the person in the picture may actually be concerned about his professor seeing the photos and not necessarily about his friends. Van den Hoven (2007) agrees this is a possibility and, therefore, refers to Michael Walzer's spheres of justice (Walzer 1983:17) for possible identification of different social spheres of access. For example, people in the social sphere may love their connections to be aware of their identity-relevant information, but will do all it takes to hide their unruly behaviour from their (prospective) employer.

4.3.3. Purpose specification and use limitation

OECD is an international body that deals with economic, social and government challenges of a globalised economy. It offers eight guidelines to safeguard privacy and trans-border flow of personal data. These guidelines have been addressed by the South African POPI Act (POPI 2009:10-16), and are, therefore, regarded as universal standards that every private organisation must comply with. As reported by Dowling (2009), the guidelines have even been a basis on which some countries (such as England, Denmark, France, Italy, Germany and Australia) built laws governing their data-processing.

The purpose specification guideline states that "the purpose for which personal data is collected should be specified not later than the time of data collection", while the use limitation guideline states that "the information should not be used for other purposes than mentioned unless with the subject's consent or the law authority" (Riphagen 2008:28). This is quite understandable, especially if viewed from the data subject's point of view. In the above example, the photographer needed to have duly informed the subject of his intent and obtained his consent to circulate the photo on an SN. He is thereby liable to purpose specification and use limitation guidelines, and deserves to be punished accordingly.

4.3.4. Least authority principle

Van den Hoven (2007:465) presents a fine-grained authorisation matrix as a way out of the challenges of information dissemination amongst different social spheres. This matrix is referred to as the principle of Least Authority (POLA) and it is adjudged to be safe, efficient, effective and easily implementable to mitigate the potential unruly behaviours. In order to minimise errors and abuse of authorities, therefore, Chris Soghoian once advised that SNs should be designed in a way that each function can only access the minimum information required for its responsibilities (Soghoian 2008:Internet).

POLA, in goals and objectives, is similar but not the same as the Principle of Least Privilege – POLP (X-byaeger 2010:1). While POLP dictates that every application and SN user should operate with the minimum privileges necessary for the roles, POLA dictates that an entity should not have authority higher than what is required to perform its responsibilities (Chizomadia 2012:5). Although both are considered best practice (and not immutable laws) to minimise the potential impacts of a successful malicious entity, POLP is particular about the first-order impacts of an entity, while POLA worries about all (Chizomadia 2012:5).

4.3.5. Restriction on moral autonomy

Users are often effectively pre-empted to represent themselves or create their own identities for other SN users. However, the likelihood of severe threat is high where, in addition to his moral autonomy being duly restricted, a user is being pre-empted from coming up with his own moral identity. This is simply because he is not in absolute control of his identity data. This may actually not sound acceptable to everybody as an excuse to protect their privacy, but Boyd (2007:17) offers a series of potential challenges behind people engaging in identity production. She maintains that human physical bodies are not applicable on SN (but their pictures and images), and that varying skills and knowledge are required to interpret and manage impressions. Hence, someone can use another person's profile to create a fake profile for himself, with the real owner not having control over his own identity.

MySpace sees identity as a social process that depends on situation and circumstances. Teenagers are more involved in identity formation, and the challenges of doing this in public have been contributing to their growths and development (Boyd 2007:16). Notwithstanding, situation and environment are key, because, for instance, the potential impacts of identity information disclosed online (on the basis of being a social experiment for growth and development) cannot be equal to when this information is disclosed to friends in a room. Victims are less concerned about the shameful information being divulged to the public but their inability to forestall the attack (Van den Hoven 2007:470). Information spreads fast on SNs as it is easily copied, permanently stored and independently searchable.

Data protection laws guard identity management and insist that the data owner should be adequately informed and fully consented with the objectives of the data processor with regard to data collected. People's perception about, and their relationship with an individual are grossly affected by the volume and quality of his information at hand. The measurement of awareness effectiveness on SNs will, therefore, be more accurate, and the process better enhanced when certain information about an individual is correct and complete.

The reasons for data protection have been further elaborated in this section, however, adequate data protection can only be achieved when awareness programmes are effectively implemented. This agrees with a survey conducted by Ernst and Young (2004), where inadequate awareness was adjudged the biggest challenge to effective information security. A technique that appears effective to resolve problems plaguing SNs for now requires users to take a more careful approach to why, what and how much data they share, and ensure these data are adequately protected. All these reasons emphasise how indispensable awareness is to SNs.

4.4. Motivation for awareness in SNs

Debates are ongoing for over a decade now at various organisations including the United Nations, emphasizing the needs for awareness. According to Wamala (2012:17), "Cybersecurity has been high on the agenda of the United Nations (UN) for a number of years. The UN took up the subject out of recognition that building trust and confidence in the use of ICTs is crucial to the socio-economic well-being of humanity. As a result, the UN General Assembly (UNGA) has expressed itself on cyber-security matters" in major resolutions including UN (2003), UN (2004) and UN (2010)".

In the same vein, SNs are changing the way we interact with our friends and customers, as well as how many internal departments are linked by systems and networks, and individuals are getting connected with numerous suppliers, partners and markets (Ryan 2011:Internet). Section 3.2 already summarises how several airlines are using SNs for their business operations. Embracing social media for business, therefore, offers huge potential, some of which was presented by Kramer (2012:Internet). MySpace is embraced by upcoming musicians in particular, to upload their songs to their own page for their potential audience to hear (Ryan 2011:Internet). This was how current pop stars, like Lily Allen, came into the limelight after posting demos of her music on MySpace in November 2005 (Ryan 2011:Internet).

Information security is crucial and worth investing in to improve the organisation's profitability. This is possible only when the number and the impact of information security breaches, as well as their direct and indirect costs, can be reduced to the acceptable minimum. Albrechsten and Hovden (2010:439) submit that these costs manifest themselves in different ways such as follows:

1. Productivity lost through time wasted in investigating and sorting out breaches.
2. Permanent loss of data.
3. Expenses incurred for data and system recovery.
4. Notification of regulators and customers.
5. Fines paid for breach of laws and regulations.
6. Reputational damages resulting to customer defections, brand and goodwill devaluation.

Availability of adequate information makes it relatively easier to take managerial decisions by minimising the error margin and mistakes (Hinson 2012:Internet). However, data protection

and value enhancement of information security may turn out to be a key strategic objective of the major SNs. Notwithstanding, emphasis on awareness amongst all other SN security techniques continues to grow. The rationale behind this growth will be discussed in the following sections.

4.4.1 Relevancies of security drivers

The following drivers, as highlighted by ENISA (2007:3), increase the emphasis placed on awareness techniques:

1. Business requirements change along with the advancement in technology use (like podcasts).
2. Foreign regulators (such as Singapore and U.S.A.) require all stakeholders of SNs to undergo awareness training.
3. Regulatory bodies in EU States are now focusing more on security.
4. The threats of organised crime continues to increase on SNs as evidenced by a survey report of Criminal Intelligence Service Canada (CISC), where malicious doings on SNs are at a high level with a rise in spam, phishing, Trojans, and zero-day threats (CISC 2010:8-46).
5. SN users are more security-conscious today, implying that negative press reports may have a considerable impact on an organisation's goodwill.
6. Identity theft is also on the increase hence, it is required of SNs to ensure that data are securely stored. A compromise on personal identity data may be costly and lead to a loss of public confidence, and litigation.

4.4.2. Technical security is inadequate

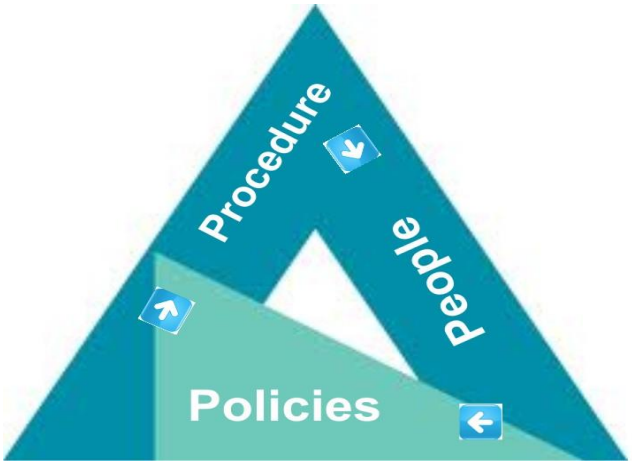
Several technical efforts have been made by many researchers to protect SNs, yet information security remains inadequate as could be seen from numerous incident reports confirming the increase in the rate of security breaches. For instance, Esma et al. (2010) introduced Privacy Watch to take care of the basic privacy criteria of SNs. Asim, Mehmet, and Abdul (2010) also proposed an API, which was eventually implemented by some SNs to automatically group friends into different social groups. Nevertheless, many users still fail to use the social circles and the applications owing to lack of user awareness (section 1.1). All these issues suggest that technical controls cannot be a total solution to privacy issues on SNs.

In November 2005 while presenting his keynote speech at the World Expo Security World Conference in Singapore, George Wang (CISO of Reuters Asia) attributed security failure to the following factors, but he failed to recognise human error, which is the main source of security breaches (Hinson 2012:Internet):

- Too much attention is given to security.
- Security measures are not aligned with business objectives.
- Communication gaps between IT professionals and senior management exist.

This implies that an SN's best defence against both internal and external breaches is not technology alone, but also the soft side – policies, procedure and people (figure 12).

Figure 12: Soft side of technology (own compilation)



Meanwhile, the owners of SNs keep on investing heavily in firewalls, antivirus systems and other technologies; each of those systems is sold on the basis of its effectiveness but yet organisations are still suffering from severe information security breaches and the problems are getting worse (Johnson 2012:18). Gartner (2011:Internet) admitted that 80% of unplanned downtime is due to people and processes. The Committee of Sponsoring Organisations of the Treadway Commission also agreed that internal controls are not only affected by policy manuals and forms, but also by people in an organisation (Johnson 2012:4).

The Global Information Security Workforce Study looked at this issue in-depth. In line with the submission of over 4000 information security professionals from over 100 countries in the largest study of its kind, Hinson (2012:Internet) reported that the following elements, arranged in order of importance, are most essential to effectively protect SN infrastructure:

1. Management support to security procedures and policies.
2. Users' adequate compliance to security policy.
3. Security staff qualifications.
4. Software solutions.
5. Hardware solutions.

The first three elements underline the need for SNs to concentrate on policies, processes and people; the soft side of technology that conventionally has been ignored for an absolute reliance on software and hardware to solve security issues. It is getting clearer to organisations that security is all about people and that security is just an enabler, not a total solution to ascertain a good security strategy (Johnson 2012:7).

"The question of whether to spend the budget on security technology or awareness, training and education highlights a false dichotomy. These are not alternatives but complementary and mutually supportive approaches. Technical security controls are strong but they have to be correctly specified, designed, developed, implemented, configured, used and maintained" (Johnson 2012:11) – all of which steps involve human beings. In other words, Hinson (2012:Internet) concluded that it is still human beings (such as security vendors, employees, management) that utilise technical security controls.

4.4.3. Reduced risk profile

Various reports of incidents in news media damaged the reputation of SNs, giving enough reasons for SN users to be more privacy-conscious. Although current SNs now incorporated privacy settings and some other privacy tools to report spam and block users, they are still safe enough to prevent privacy risks (Esma et al. 2010:172). This implies that even if SN users have control over their own profile, they do not have control over their information revealed by others, hence information can be fraudulently disseminated without the owner's consent.

A survey carried out by PriceWaterHouseCoopers in 2008 on Internet Security Alliance rejects risk analysis and intelligence-gathering as security factors but infers that technology – identity management, firewalls, and intrusion-detection system – has been the enabler of security so far (ISAl 2010:12). Investment in security must, therefore, be diverted from IT to risk analysis and mitigation in order to take care of the human element in information security

(PriceWaterHouseCoopers 2008:17-19). All these assertions are suggesting that the total risk profile on SNs can only be minimised with adequate and effective implementation of awareness.

4.4.4. Regulatory compliance

Information security is no longer limited to usernames and passwords. Legislation and regulatory bodies and various privacy/data protection laws have started saddling organisations with security responsibilities. This explains why some organisations are still being funded by some regulatory bodies to implement sound information security policy programmes. Such regulatory bodies include: Health Insurance Portability and Accountability Act (HIPAA) of U.S.A; Gramm-Leach-Bliley of U.S.A, Basel II of Switzerland, Sarbanes Oxley Act (SOX) of U.S.A., Federal information security Management Act (FISMA) of U.S.A., and the Independent Communications Authority of South Africa. The Electronic Communication and Transaction (ECT) Act of South Africa, and the Electronic Communication Act (ECA) of South Africa are typical examples of laws that guide an organisation's compliance.

During the last ten years, regulators have passed several state, federal (Info 2011a:Internet) and international (Info 2011b:Internet) regulations, most of which are particular about information security Regulators such as the U.S.A. and the United Kingdom (U.K.) are also expecting much from staff in terms of awareness training (ENISA 2007:3), thereby necessitating organisations to start adjusting their information security policies in line with legal and regulatory requirements. Some regulations like ECT and ECA, emphasise the conditions for written security and privacy policies, while others like FISMA are only interested in how good the security is for the organisation. In any case, auditors and other enforcement agencies are required to strictly adhere to accepted frameworks or best practices, all of which still necessitate written policies.

Info (2011b:Internet) outlined some privacy-related regulations and their respective information security policy requirements in one of their publications in 2011. This list is summarised in table 5 and where necessary, it presents security policy requirements for some key frameworks used to manage regulatory requirements. However, the study could not find policy requirements for any of the African regulatory bodies.

Table 5: Regulatory requirements for security policies (adapted from Info 2011b:Internet)

Regulation/Framework	Industry/ Country	Policy requirement
HIPAA (Health Insurance Portability and Accountability Act of 1996) Security Final Rule	Healthcare (U.S.A.)	Appropriate and reasonable policies and procedures are to be implemented to ensure adequate compliance with the standards or other requirements.
Sarbanes-Oxley Act, Section 404 - based on COBIT, section 6: Communicate Management Aims and directions.	All publicly traded companies (U.S.A.)	Management should be fully responsible for developing, formulating, documenting, promulgating and controlling policies covering general aims and directives.
New Basel Capital Accord (Basel II)- Quantitative Standards, Section 606	International banking	The risk management system of a bank should be adequately documented. The compliance of the operational risks must routinely be checked against the approved policies and procedures.
Gramm-Leach-Bliley Act Title V - Section 501 Interagency Guidelines Establishing Standards For Safeguarding Customer data.	Financial services (U.S.A.)	A detailed written information security policy should be implemented by each bank and must include physical, technical and administrative safeguards.
FERC Cyber-Security Standard. CIP-003-1 Security Management Controls	Energy/Infrastructure (U.S.A.)	A cyber-security policy has to be established and maintained by the responsible entity to address both the standard requirements and the cyber-security controls governance.
Federal information security Management Act (FISMA). NIST SP 800-26	Federal Government (U.S.A.)	The effective implementation and maintenance of information security policies, procedure and control techniques shall be delegated to the CIO by the head of each unit in an organisation.

Regulation/Framework	Industry/ Country	Policy requirement
PIPEDA (Bill C6) – Personal Information Protection and Electronic Document Act	All industries (Canada)	Policies and practices shall be implemented to give effect to the principles. Organisation shall be objective regarding the management of personal information.
EU Data Protection Directive	All industries (EU)	Technical measures adequate for personal data protection must be implemented by organisations.
ISO/IEC 27000 and ISO/IEC 27001. Section 1.1 information security Policy Document	Security framework	All employees in charge of information security should have access to written policy document.
GAISP – Generally Accepted information security Principles, Version 3.0. Section 3.1 information security Policy	Security framework	Management shall develop and maintain policy and supporting standards, baselines, procedures, and guidelines to address all aspects of IS.

4.5. Awareness raising techniques

Information security specialists are of the same opinion now that security relies more on people than technology (Bell 2010:1), and that employees present bigger threats to information security than outsiders (Koremans 2010:Internet). A study conducted by the Ponemon Institute in 2012 about 700 IT security practitioners discloses that almost 80 percent of survey-takers stated that negligent, malicious employees or other insiders were responsible for a minimum of one data breach within their organisations over two years (Trendmicro 2012:2). It then follows that security improvement is a function of improved beliefs, attitudes and behaviour of both individual and groups. This theory is often referred to as a conventional approach, and confers so much in IS expansion and enhancement.

4.5.1 Conventional techniques

In a seminal paper published in 1993, Michel Kabay discussed the psychological rationale behind the failure of conventional approaches towards awareness development. His argument was simple and straightforward because his methodologies centred on human schemas, even

though most schemas do not always comply with security policies and procedures (Kabay, 1993:2). He defined schemas as "a self-consistent views of reality that helps to pay attention to what users expect to be important and to ignore irrelevant data". For example, a normal schema or expectation in a server room includes a cool environment, displaying of policy guidelines, security discussions, telecommunication challenges, and smart winter dress. It is not expected to be characterised by physical fights, staff dressed in a swim suits or coming into the room with drinks and food items. Schemas make people behave somehow in a given situation as explained by Kabay (1993) in the following examples:

1. In a normal office setting, it is a common employee practice to share tools and devices such as rulers or staplers, trust every team members and divulge information, or even leave paper documents wide open, especially when not in an exclusive environment. However, sharing user IDs and passwords, disclosing information to unauthorised persons, and leaving systems logged-on unattended are gross breaches of information security schemas.

2. Courtesy demands that someone should hold a door open for his colleague who is fast approaching the same door he has already opened. Visitors are also expected to be welcomed with a gentle smile because he may be a (potential) customer. However, normal politeness teaches that the CEO should have unrestricted access to everything within his company, whereas IT operators and database administrators are trained not to attend to anyone without due authorisation processes and necessary documentation.

3. Schemas often negate which information users do remember. Kabay once declared that, "when information inconsistent with users' preconceptions is mixed with details that fit their existing schemas, they selectively retain what fits and discard what conflicts". For instance, if people have read several novels or watched series of movies demonstrating the assertion that hackers are the major information risks, they will find it difficult to remember and accept the truth that information security user attitudes and behaviours are more dangerous than threats from outsiders (Kabay, 1993:3).

The awareness programme implementation must therefore engage non-rational (non-conventional) methods, and colleagues' imagination and emotion must be appealed to as well. There should be a commitment to security and not just a mere description.

4.5.2 Non-conventional techniques

Currently numerous non-conventional awareness-raising techniques have been identified (Brodie 2009:5-8; ENISA 2007:8-13; Heidari 2010:10-16; Hinson 2012:Internet), most of which are used

in combination with another; all to achieve the desire to keep costs to the minimum while increasing profits. These techniques include, but are not limited to, the induction process/ appointment letter, security policy/staff handbook, regular emails or newsletters, computer-based training (CBT), leaflets, intranet sites, quizzes, promotional materials (e.g. pens with the company logo printed on them), etc. Each of these awareness initiatives requires senior management support to be effective and command respect.

A formal security policy remains the backbone for the information security awareness framework, without which it would be difficult or even impossible to ensure good behaviour (ENISA 2007:8). A good practice standard is an epitome of an organisation-wide security policy. For instance, ISO/IEC 27001 is a standard that postulates training and awareness programmes in every organisation, and many other standards also call for user-awareness training to encompass security policy. Meanwhile, risk analysis is one of the major components of information security policy and awareness training, and it is meant to give room for policy formulation and training development. Hence, investments will be most rewarding and effective in business and information security when it is channelled towards users training in IS and network security (Johnson 2012:15).

4.5.3 Information security awareness techniques

Most standards advocate a formalised approach for awareness and present the following reinforcing elements as parts of a normal virtuous circle (ENISA 2007:8-9):

1. Requirements analysis: Management is required to pinpoint the training needs of each staff member, and enlighten its staff about the security policy relevant to their job functions. Several standards have outlined control topics to encompass spyware, virus outbreaks, and strong passwords.

2. Training is tailored to users' responsibility: Every staff member including contractors must be adequately trained in line with their functional roles, and always be enlightened on the processes required to implement security in their daily activities. Policy changes in their functional procedures should always be communicated to them.

3. Ongoing review: The contents of awareness programmes must always be reviewed to remain current, and the effectiveness of these programmes with regard to both the participants and the organisation must always be measured.

Some information security surveys (Continuity 2006; Infosecurity 2012), including the information security breaches survey of the U.K. Department of Trade and Industry (DTI), established the following:

1. Many organisations are now meeting their responsibility of raising awareness amongst their staff, by organising awareness training to new employees and incorporating security responsibilities into their staff handbooks.

2. Most organisations are involved in educating employees about their security responsibilities.

3. If the information security is of higher priority to the senior management, the company is more likely to place higher priority on staff education.

These studies are consistent in that each of the respondents applies at least one technique to raise user awareness to their security responsibilities. These techniques are less expensive and, therefore, popular. Although, they are convinced that policies, handbooks and guidance can provide basic foundation to awareness-raising (ENISA 2007:11), some respondents disagree in total that the techniques cannot be effective on their own, as it is practically and logically impossible for every staff member to acquire all required information for adequate awareness.

Although classroom training is the most effective of all, not many organisations send existing staff for continuous training. This could be attributed to cost and time factors. Many organisations find it extremely difficult to allocate sufficient time to training needs, while the supposed cost of arranging and running these courses could be daunting to others. The latter could be an issue, because even though organisations give high priority to Information Security, many of them cannot justify their expenses on awareness programmes (ENISA 2007:9). In ENISA (2007) research for instance, "only a third of respondents could put up a formal business case to justify their expenditure". In the absence of a convincing business justification, organisations are often constrained to take the essence of improved awareness as intangible and unquantifiable. Consequently, they treat the training budget as an overhead rather than an investment and a compliance requirement. Therefore, the effective awareness programme that ranked highest in this context of cost implication appears to be that which targets a limited classroom training budget, which is more likely to be low and easily justifiable.

4.6. Impacts of awareness programme

This chapter established reasons behind a security investment moving from the technology-operation-based to a risk analysis and mitigation philosophy. It implies, therefore, that it is

much easier and safer to do preventative security rather than reactive security measures, necessitating awareness and education as the keys to solving this issue. Accordingly, this study aligns its arguments to Hinson's (2012) proposal that an awareness programme, if well planned and coordinated, will provide adequate security to the organisation's information assets by accomplishing the following:

1. Putting under management control a series of awareness, training and educational measures.
2. Providing a framework to manage and evaluate IS, as well as various tools and techniques for effective communication.
3. Smoothing the process of punishing those that do not meet their information security obligations.
4. Making the application of information security controls more stable and reliable.
5. Making information security controls more effective by employing only improved controls or security.
6. Meeting the legal obligations of the organisation, as regards the awareness enforced imposed by some acts (FISMA, HIPAA, and SOX).

4.7. Summary

This chapter justifies the need to measure awareness in SNs. It discusses the basis for securing SNs and emphasises that the network owners, in addition to having adequate awareness, should always shoulder the responsibilities of providing a privacy-enhanced environment to the users. In which case, SN operators must come up with an incentive to motivate their staff and users towards secured behaviour and performance. With the proper application of various recent research studies, the chapter was able to address the question of "why an awareness technique is a must", and in particular research question 2, by singling out awareness as a major control technique available to measure security in SNs.

It is established in this chapter that researchers have been channelling some notable efforts towards raising awareness techniques lately. Studies of Brodie (2009), Hinson (2012), and PriceWaterHouseCoopers (2010) were reviewed to identify some notable techniques that are specific to raising awareness in SNs. In the research conducted in 2007 by ENISA, training was adjudged the most effective technique, although it is very unlikely to be cost-effective. However, training may not be effective without staff/user motivation, and senior management

support and involvement. While it remains a fact that raising awareness in SNs depends on an established principle of human behaviour (beliefs, attitudes and behaviour), the chapter presents enough psychological reasons why the conventional approach cannot be effective in raising awareness. If the awareness programme relies strictly on factual information about risks and proposed policies and procedures (conventional methods), they are very likely to run up against human refusal to act logically.

Security awareness efforts are the first line of defence, but Van Niekerk and Von Solms (2004) maintain that these efforts, though important, are insufficient to give the desired results. This is in line with the submission of Stephanou and Dagada (2008:3-4) that it is still possible for messages communicated to users to be ambiguous and confusing, particularly in dynamic complex threats such as phishing attacks, despite the understanding that awareness is important. Given the prediction of present and future development, the implementation of an awareness programme cannot guarantee that the guidelines are being understood and complied with by every audience. It is, therefore, important, to measure the effectiveness of a method towards achieving its purpose and objectives.

CHAPTER 5 AWARENESS MEASUREMENT IN SNs

5.1. Introduction

Researchers and managers are always confronted with two distinctive challenges when it comes to developing a measuring tool and performing the measurement. These challenges have to do with what to measure and how to measure (Kruger & Kearney 2005:3), which are parts of the independent variables to this study (section 2.3.2) and are being promoted by certain requirements such as sustainability, ease of use, and the use of scientific methods.

This chapter will address these problems by defining the needs for absolute measurement and evaluation of effectiveness of awareness techniques from individual perspectives. Factors used to measure awareness effectiveness in SNs will be identified and extensively reviewed, to put to rest several speculations on how and what to measure in SNs. Considering an assumption that expert opinions are not often accurate, it is more desirable to measure the impact of awareness programmes. Hence, this chapter will evaluate some awareness benchmarking and metrics in relationship to their myths. Some awareness measurement techniques will be reviewed, and the best approaches to measure the awareness efforts on each of the SNs will be discussed.

5.2. Background

Even when an awareness programme is successfully implemented with adequate top management support, organisations still cannot be sure that every stakeholder understands his security roles and responsibilities (Singh & Patterh 2007:331). While it is difficult and uncertain to assume the success of any security effort, it is pleasing and more assuring to often measure the status of every awareness programmes on SNs. Hence, a more structured approach is always required to study the impacts of awareness techniques on SNs in order to ascertain its contribution to the field of security (Kruger & Kearney 2005:291).

There is a unique dilemma with information security professionals; they hardly get recognised when nothing goes wrong with their job. This position is not only demoralising but also put them in a difficult position when vying for resources or presenting a business case to justify their budgeted expenditure (Chapple 2005:1). It similarly suggests that information security is not duly recognised until the occurrence of an attack; and may be a fundamental reason why

management had hardly shown any interest in evaluating and measuring the impact of information security until 2007 (Singh & Patterh 2007:341).

Most professionals appreciate metrics to measure their performance (Jithin 2012:Internet). For instance, business leaders measure marketing efforts by the revenue targets they meet, and network administrators' performance is a function of the targeted system availability and uptime guarantees. There is a need to set a measurable target for information security professionals as well, to accord information security the respect and attention it deserves, and more importantly to signify management interests in ensuring the implemented security and controls are effective as intended.

5.3. The need to measure awareness

While the purpose of a typical SN is to make money by promoting interactions and allowing millions of people to stay in contact, the objective of each individual or organisation buying into SN varies. Some use them for business goals, to network and make new deals, while others use them purely for personal reasons, not even aware of the business opportunities in the SN's environment. This implies that just as awareness, SNs are all about people, who remains the weakest link (Bangkok 2010:Internet; Boss 2007:27; Van Niekerk & von Solms 2004:2) and the most significant component of all (Johnson 2012:4). In this section, people are regarded as employees or users of the SNs and this explains why the measurement and assessment of awareness is always a function of the success of education and training efforts. This section only summarises some motives why awareness measurement and assessment are a must.

1. More security courses are being offered now at universities and other institutions but their coverage is limited to specific needs. An assessment effort will highlight this shortcoming and help further to tailor courses and academic programmes toward all areas of need (Yngström & Jörck 2010:4).

2. Every normal individual at a certain stage in life makes concerted efforts to improve his knowledge for an improved living, not necessarily only at a financial level. Assessment of training courses and programmes will guide management to sustain or improve on the quality of knowledge being transferred. This improved training program, in turn becomes a source of attraction to other individuals interested in information security education, thereby improving their knowledge as well (Yngström & Jörck 2010:4).

3. SN like other organisations does take the security status of an investment or process very seriously when making investment decisions.

4. The security status of an investment or process is of utmost importance to SNs when making investment decisions. However, security importance can only be appreciated when implemented security is well evaluated and effectively measured. It is, therefore, required that, for management to take into account the varying costs and income arising from this efforts, investments in education and training should be measured with a reasonable return on investment (ROI).

5. People's feelings and perceptions dictate their behaviour and attitudes. However, these attributes can be influenced when critical security components are measured towards developing strategies for continuous improvement (IWS 2007:Internet) in the following ways:
   - Management tends to understand security better and offer more support.
   - Cost reduction is accomplished through some improved efforts like the implementation of an effective virus control policy.
   - Baselines for all the ongoing improvements, including internal controls on the SNs, are developed.
   - Accountability for managers and supervisors especially with respect to the SN user requests, support and management.
   - Employee relations are enhanced by co-opting them into the internal and external processes.

5.4. Measurement of determinant factors

Based on Chapple's (2005) submission, this section will classify the factors that can help in measuring the effectiveness of awareness in SNs into three basic areas – audit results, lost productivity, and user satisfaction.

5.4.1 Audit results

Audit results are always a good starting point of measurement. An audit exercise is usually periodic, and its results do not only help to measure an organisation's preparedness against potential attacks or security incidents, but also suggest measures for an improved information security operation (Chapple 2005:2). For instance, the unauthorised posting into a post-no-debit account of a bank highlighted by an auditor is an indication that the automated preventive

controls to prevent such transactions are not effective or are not in place at all. Similarly, gaining unauthorised access into someone else's personal data even when the latter has put in place all the necessary private settings indicates that the privacy control is defective. Hence SN, in the real sense of it, is not prepared for such a breach of control attack, even though it is clearly stated in its policy document. However, the result is a good justification for such an organisation to invest further in terms of security.

Auditing could be internal or external and can be automated or manual or both. Some security utilities have been around for a while to measure, for instance, the vulnerability of workstations or servers to potential attacks. Nessus, the Centre for Internet Security (CIS) benchmarks, and the Microsoft Baseline Security Analyser are epitomes of good security tools (Chapple 2005:2). Therefore, while carrying out an IS audit, a security scorecard may ultimately be used to track changes on SNs. For instance, SNs set a passing score as a CIS standard for performance evaluation and measurement. If the percentage of workstations with a score higher than the CIS benchmarks is low, there is a need to improve on workstation security, otherwise, workstation security is adequate and effective.

5.4.2 Lost productivity

Lost productivity is one of the measures used in IT organisations to estimate the effectiveness of maintenance programmes. While lost productivity could arise from the workforce end, such as a strike, sickness or employees taking longer than the allowed lunch break, it can also be traced to inadequate employee awareness. A particular instance is the use of rate of virus outbreak to determine the success of awareness efforts, or using time involved to come back into operation to determine the effectiveness of awareness training on disaster recovery exercise or business continuity planning.

These same metrics will be handy when determining the total loss owing to the occurrence of information security issues or challenges (Chapple 2005:3). The time taken to resolve virus attacks, for instance, is a good measure of awareness efforts as it is expected to take a minimum avoidable number of hours. If SN is properly taking note of its productivity loss in every aspect of it, some awareness issues will be obvious, and these may eventually be used to measure the effectiveness of the site. Additional resources may need to be diverted to strengthen the information security efforts if the issue is momentous and can result in a significant loss of productivity.

5.4.3 User satisfaction

The success of any information security effort revolves primarily around the users and their transactions (Bell 2010:1; Chapple 2005:3). Therefore, the extent to which users are satisfied with awareness efforts should be a metric to consider when measuring the effectiveness of awareness efforts (Kramer 2012:Internet; Ryan 2011:Internet). To this extent, a questionnaire may be sent to SN users for possible answers to some sample questions such as:

1. To what extent were you satisfied with the services you received?
2. Was the solution effective or defective to your problems?
3. Did the solution influence your ability to perform your job functions?

When satisfaction scores are broken down by service type, an SN might be enabled to figure out shortcomings in a particular awareness effort. A low score is an indication of a weak awareness programme and may call for additional resources. However, to emphasise its importance, some organisations do consider these scores for staff evaluation and performance. The reasons may be traced to the fact that these results are very easy to measure or determine the success of a programme because supervisors generally understand and appreciate customers' satisfaction.

5.5. Problems in measurement

Measuring impacts of information security education and training is an indirect way of measuring a change in human behaviour in relation to its impact on the SNs. Many associated challenges make the measurement so difficult to achieve, just as it is in risk evaluation and management. Some of these popular challenges include the independent variables such as how to measure the lack of incidents, differentiate between what people say and what they do, and interpret the numbers.

5.5.1. Measuring the lack of incidents

If the information security risk of an SN analysis is accurate and effective information security controls are implemented, the number and severity of security incidents are expected to reduce. Similarly, if the number and severity of incidents are measured, there will be some numbers/figures to work with. That is primarily the goal of information security (Hinson 2006:2), and then follows that:

1. If the rate of incident or the numbers and severity of incidents are lower than before the implementation of awareness programme, the organisation can claim success. A good example was the occurrence of fewer website defacements since 2006 compared to ten years earlier (Hinson 2006:2). Meanwhile, it is possible that an organisation has not done anything to improve control and coincidentally control failures are not being reported again. Although this could be attributed to the fact that sites are better protected now (control improvement), it is equally possible that the number of hackers actively targeting site defacements (threat reduction) has reduced for whatever reason.

2. Again, a rise in the number and severity of incidents is not necessarily an indication of an ineffective control. It may perhaps suggest that an organisation has failed to keep abreast of the growth in threats and impact.

However, the challenge here is conjecture. It is difficult and almost impossible to objectively evaluate and measure what could have happened if an effective awareness control were not in place (Barry 2012:1).

5.5.2. Discrepancies between what people say and what they do

Employees could attain an awareness level measurable to information security regulations, through an information security training and education programme. Yet, it does not necessarily mean that they comply with these values or rules (Johnson 2012:13; Yngström & Jörck 2010:18). Similarly, being fully aware of the measurement exercise, some employees may choose not to give the true position of their awareness levels because they are not sure how their employer will take it if they disclose their ignorance of the rules and regulations that are supposed to be their guide. From an SN's perspective therefore, the emphasis should not be on a user's knowledge (what he knows) about, but on what he does with this Information Security knowledge.

5.5.3. Interpreting the numbers

Interpreting the numbers is another problem associated with measurement. It is difficult putting numbers or figures on issues like awareness because they are considered to be a soft issue (Yngström & Jörck 2010:18), however, exact numbers are hardly required to form an opinion. For instance, if the awareness level is roughly 70% it may still be difficult to determine whether the security is good or bad. Once numbers are produced while measuring

soft issues, the numbers might be very difficult to interpret as the contexts have to be made clear (that is whether the organisation is an SN, bank, or fast-food chain).

5.6. What to measure

Some studies have been focused on what users believe and do about security in the real world. At the same time other studies have focused on security in the organisational context, having in mind requirements of the organisation and user participation to support compliance (Veseli 2011:15). Kruger and Kearney (2005) gave an example on developing a model for measuring information security awareness, and this model was applied in an international gold-mining company, with the goal to monitor changes in security behaviour. As a result they revised or repeated awareness campaigns, whenever they identified the need for it to happen.

What to measure is crucial, but in practice, it is difficult to identify the right metrics (Hinson 2006:8). Security measurement is all about common sense; managers must know what to measure, arrange them in a meaningful and manageable order, and come up with a repeatable formula to disclose the security status, and how this status changes over time (Lindstrom 2012:Internet). The seven myths (section 5.8.2), as well as some of the following rules of thumb, need to be taken seriously when considering what to measure.

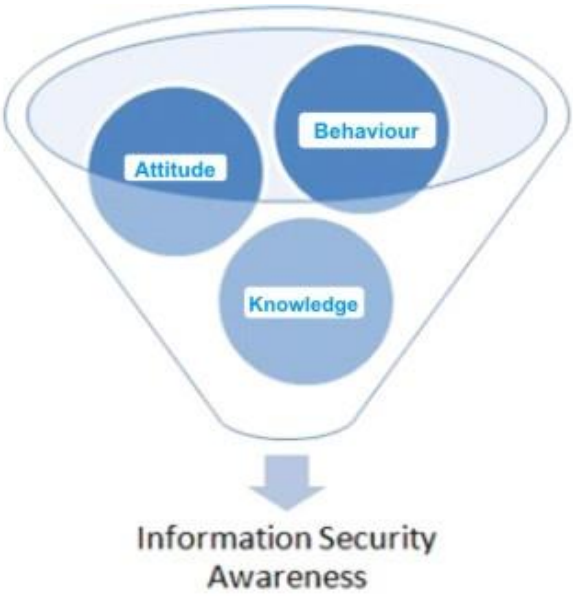
1. A measurement process should not be implemented if it will not be followed routinely and systematically. Repeatable and reliable measures are absolutely needed.
2. An organisation should not capture data that they do not intend to analyse. Such a cost is therefore avoidable. This is also not allowed according to the POPI Act (2009:10-16).
3. Data should not be analysed if the organisation would not make practical use of the results.

It is assumed that organisations can achieve so much in terms of measurement and security without elaborate processes or expensive solutions. For instance, the amount of time that an IT service is fully available for business use, expressed as a proportion of the time needed, can be a true measure of system availability. The IT department must have measured the percentage uptime for key IT services, especially if there are contracts or services under service level agreements. However, uptime calculations often overlook some non-availability conditions such as maintenance and planned downtime (Hinson 2006:8). This cannot be true unless when these conditions do not occur within the agreed service limit.

5.6.1. Knowledge, attitude and behaviour (KAB)

Generally speaking, when classifying what to measure, there are three dimensions that should be absolutely considered. That is, knowledge (which focuses on what an employee knows); attitude (which focuses on what an employee thinks); and behaviour (which focuses on what an employee does) (Veseli 2011:15). Research objective 1 of this study elaborates on this. Figure 13 presents a funnel of these dimensions. As applied in the Venn diagram, an SN will be better secured when the user's KAB is tailored towards the security requirements and objectives (Lacey 2009:11).

Figure 13: Dimensions of awareness (adapted from Lacey 2009:11)



Knowledge: It is important because a user cannot put security intention into action without the necessary knowledge and understanding, even when he/she believes security is important.

Attitudes: Unless users have a strong faith in security, they are not going to work securely regardless of their knowledge and understanding of security requirements (Lacey 2009:12). Attitude is a dimension that signifies an employee's disposition to act.

Behaviour: Regardless of his knowledge, an individual is not going to impact security unless he exhibits some secured behaviours.

From a user's angle, security generally is a combined function of knowledge, attitudes, and behaviours. Therefore, for SN managers to be sure that their awareness training is effective, they need to measure the impact on these three elements. Lacey (2009:12) later subdivided these dimensions into the following six focus areas:

1. Focusing on the policy of the company.
2. Keeping passwords and personal identification numbers secret.
3. Using internet and email carefully.
4. Using mobile equipment carefully.
5. Reporting incidents like viruses, theft and losses.
6. Being fully aware that all actions carry consequences.

5.6.2. Attitude and subjective norms

Khan et al. (2011) employed the Theory of Reasoned Action (TRA) to appreciate the change in behaviour and attitude, and the resultant impacts of change in the latter over the former. This theory, as represented in figure 14, relates attitude to behaviour, and encompasses both the direct and indirect attitude-behaviour paths (Farrior 2005; Fishbein & Ajzen 1975). Behavioural change is a function of individual intention, which is easily influenced by two main factors – attitude and subjective norms (Farrior 2005). The attitude describes what an individual likes or dislikes whereas the subjective norm is the individual's belief of doing exactly what people think about him.

Figure 14: Model for measuring awareness (adapted from Khan et al. 2011:10864)

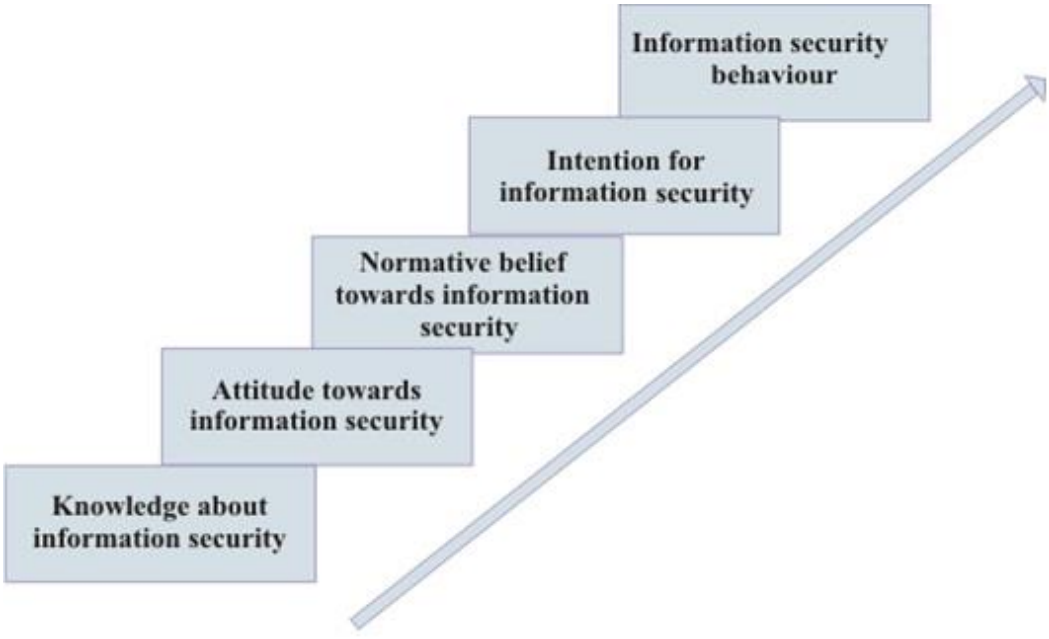


Figure 14 presents Khan et al. (2011) model to measure and evaluate the impacts of awareness efforts. These steps, arranged in ascending order, include knowledge about Information Security, attitude towards Information Security, normative belief towards Information Security, intention for Information Security, and information security behaviour. The model considers

knowledge as its backbone and combines this knowledge (from the attributes of the KAB model) with social norms (from the theory of planned behaviour) to attain the required change in user behaviour.

Table 6 presents seven formal and informal instruction methods of awareness, along with their respective effectiveness in the measurement and evaluation model**.** In the table, S/N is the serial number arbitrarily selected by the author. The 'Y' or 'N' mark denotes the presence or absence of such component in the respective awareness campaign tools and techniques. The total effectiveness of a particular campaign technique is determined by the total number of 'Y' marks in its row. The more model elements are contained in an awareness technique, the more it is considered.

Table 6: Awareness methods to measure effectiveness (own compilation)

S/N	Awareness tools and techniques	Component of know-ledge	Component of attitude change	Component of subjective norm	Component of intention	Change in behaviour	Overall effectiveness
1	Education representation	Y	Y	N	Y	Y	4
2	Email messaging	Y	Y	N	Y	N	3
3	Group discussion	Y	Y	Y	Y	Y	5
4	Newsletter	Y	Y	N	N	N	2
5	Video games	N	Y	N	Y	N	2
6	CBT	Y	Y	N	N	N	2
7	Posters	Y	Y	N	N	N	2

5.7. How to measure

A big challenge faced by banks, SNs, and some other organisations has been how to measure the adequacy and the effectiveness of their awareness programmes (ENISA 2007:17). Ordinarily, SNs often like to measure the shift in an individual's behaviour, which is extremely difficult to evaluate quantitatively. However, given that measurement is vital to pursue training efforts at weak areas, Davis (2008) worked on the key performance indicators (KPIs) and practical metrics to isolate conventional from unconventional methods of measurement. Unfortunately, none of these methods are non-statistical; they are all incident-driven waiting for a success of an attack or occurrence.

5.7.1. Conventional methods of measurement

Measuring three intangible dimensions such as knowledge, attitude and behaviour may appear to be a challenging task. Davis (2008:9-14) published some of the most effective methods, which help to measure the employee's awareness. These methods are presented in table 7, and the mapping is based on the theory postulated by Davies (2008). As illustrated, different methods should be used when measuring impacts of the awareness programme. When measuring attitude for instance, the best result that one can get is to use surveys, interviews, or focus groups, depending on the SN's needs, taking into consideration the number of the employees, working effort, time, and costs (Davis 2008:13).

Table 7: Conventional methods to measure intangible dimensions (own compilation)

S/N	Intangible dimensions	Conventional methods
1	Attitude	Interviews, focus groups and surveys
2	Knowledge	Assessment tests
3	Behaviours	Behaviour measures, surveys, interviews, and focus groups

Interviews are used for collecting qualitative data. The participants are allowed to answer the open-ended questions without limitation on the time and scope. The major advantage of interviews is that one can obtain useful data about items that are not easy to come by (e.g. feelings, emotions, and attitudes). However, researchers who used interviews felt that using a more open-ended instrument allowed the researchers to obtain ancillary information that would not present itself using a written survey (Kelleher, 1984:5).

Since SN users are scattered all over the world, profile groups and information categories (table 14) are conventional methods used in this study to collect interview data regarding the KAB and the sharing intentions of participants. This is necessary to determine their (KAB and intention) possible influence on the result obtained when measuring awareness efforts with an approach that is not necessarily based on incident statistics.

Focus groups are in the form of group interviews that are realised in a communication between the participants in order to gather information. This method is convenient to gather data from several participants simultaneously. The interview will be organised using cluster sampling methods over the population size, based on their locations and time zones. Awareness-raising contents may be provided in the form of a number of quiz templates. The template may be

implemented as a web quiz. Each quiz will come with introduction text, included on the same page as the question. The quiz template will be mailed only to users with weak passwords, asking them for responses.

Surveys are considered to be an excellent tool, for drawing out information from large number of participants, and to make possible the identification of broad tendency. Surveys may and may not be internet-based. The advantage of choosing internet-based surveys is that it makes possible statistical analysis of the results, and comparing the results with different groups of participants. Two surveys may be required in some cases. In this study, the survey is presented in a questionnaire form and administered as a quiz template only to users with a bad password combination to determine the possible impacts of KAB on the effectiveness of the various awareness programmes implemented.

Assessment tests and behavioural measurement are methodologies considered handy to measure knowledge and behaviour respectively. However, the review of these methodologies is beyond the scope of this study.

5.7.2. Unconventional methods of measurement

Several unconventional methods that have merit are now available to study and measure the awareness of users of SNs. Few of them, already identified and used by some researchers, are as mentioned below:

1. **Social engineering** can be used to obtain user passwords, as in Mataracioglu and Ozkan (2010). The researchers made use of phone calls to exploit employees' good faith towards seizing their sensitive information. They were able to establish that the employees in Turkish public agencies lack awareness and they also compromise the information security principles.

2. **Software** can be implemented to examine network traffic for PII that is being transmitted unencrypted over a university campus network, as reported by Briggs (2009). "The Symantec data prevention (DLP) software searched emails, files, databases, and the institution's websites for confidential data, including credit card numbers, social security numbers, and other designated information. Monitoring outgoing and incoming email for security violations entailed looking for clues in the email that might reveal sensitive data" (Briggs 2009:1) The software eventually found and flagged a social security number in an outgoing email and a credit card number in incoming mail.

3. **Worms** could be created to test the user's ability to detect phishing attempts as detailed in Meister and Biermann (2008) and Owoade and Jacob (2013). In the study of the latter, an automated worm was launched on the server of a manufacturing company to search the inbox, sent items, and address books in order to locate as many email addresses as possible. The worm sent messages to each of the emails, pretending to be the email provider and advising the potential victims of opening the attachment to correct purported errors in their email account. The number of users who cared to confirm the source of the mail by discussing the issue with the network administrator before opening the attachment was used to determine the effectiveness of the awareness efforts.

4. **Gaming software** can be used to aid in annual awareness training as reported by Cone, Irvine, Thompson and Nguyen (2007). The software can also be used to disseminate awareness information and to test the participant's knowledge after completing the scenarios. Nagy and Pecho (2009) also tested Facebook users' ability to detect phishing attacks by attempting to friend as many unknown people as possible, using gaming software.

5. Endicott-Popovsky, Orton, Bailey and Frincke (2005) equally used a **Google Hacking competition** to show local Seattle businesses how much PII was publicly available on the Internet. They used this event to promote awareness in the Seattle area.

5.7.3. Security metrics of measurement

Metrics are very good measures of security effectiveness, hence, most organisations have started using a combination of several metrics for effective measurement (ENISA 2007:17) because it affords them the opportunity to come up with a balanced scorecard for their awareness programme. In this case, decisions are not restricted to a single measure but to the basis of the overall picture. Hence, the following metrics are being considered effective enough to measure the success of awareness efforts in SNs:

1. Rate of security incidents owing to human error
2. Cost of security incidents owing to human error
3. Audit findings
4. Results of staff surveys
5. Tests of staff compliance to policies and procedures
6. Number of staff members that complete awareness training
7. Qualitative feedback from staff members
8. Volume of visitors on security intranet site

9. Rate of system downtime due to human error
10. Scan results on viruses and unauthorised software
11. Number of leaflets/policies distributed
12. Return on investment (ROI)

In the study conducted by ENISA (2007) where a range of dissimilar metrics was employed to determine how effective awareness efforts were, internal protection measures were overall the most popular. Two thirds of the respondents used audit reports and close to one-third used software crack reports, but the use of some other possible metrics was hardly noticed. The audit exercise could be carried out by the internal/external team or a third party, however, the auditor's objectives must be clear and their approach systematic for their reports to carry weight.

The second most popular metrics are adjudged to be effectiveness and efficiency measures, where participants invoke their security incident experience. Very few respondents exploited some kind of attack resistance metrics however, metrics relating to security incidents owing to human error are most common (ENISA 2007:17), as over 50% of the respondents use at least one of them. The proportion of respondents using process improvement measures is low, even though the measures can easily be captured (ENISA 2007:19). Respondents seem to prefer using awareness activities to measure changes in people's behaviours. Hence, only a significant minority appreciates input metrics such as number of leaflets distributed and number of visitors to intranet sites. The only commonality amongst them are the quantity of staff on training, as well as the staff qualitative feedback, and less than a third of the respondents even employed either of them.

In total, there was a good meeting point for metrics adjudged most effective and those adjudged to be popular, hence, respondents were able to agree on the most effective measures but only in areas where good practices were encouraged. The respondents appeared to have acquired some experience in the past which, in turn, guide their present thinking and doings. However, the majority conceded that they were persistently enhancing their approaches as they still had much to learn from the present practice. The overall result did not signify any noticeable difference across the sectors, implying that what is found effective for every individual across industries is almost the same with the exception of financial services and airlines that will not employ incident statistics metrics such as costs of incidents.

5.8 Awareness benchmarking and metrics in SNs

While awareness has to do with people appreciating the needs for security and that security is the responsibility of all, its measurement has been found helpful to identify errors and irregularities. Metrics are important and effective tools that are used to determine awareness and training needs on the SNs. According to Wilson and Hash (2003:17), metrics monitor the accomplishment of the awareness and training programme goals and objectives in three ways by means of the following:

1. Quantifying the level of implementation of awareness and training as well as their effectiveness and efficiency.

2. Analysing the adequacy of awareness and training efforts.

3. Identifying possible improvements.

Metrics are tools specifically required to measure progress towards a goal. A good awareness metrics programme is similar to car brakes; brakes make a driver to slow down but they also make it possible for him to go much faster (Hinson 2006:Internet). It takes time to set up metrics programmes, but once established and working well, it can save time in the long run by making programmes more effective. However, metrics, being the only way to evaluate the effectiveness of an awareness programme, remains one of the challenges facing awareness (lspitzner 2010:Internet). It appears to be one of the weakest areas of awareness and information security in general, even though there is no established statistics yet to argue it. This could be attributed to a view that researchers are yet to come up with a proactive approach to measure awareness. Hinson (2006:Internet) reported a small group of potential metrics that might need to be monitored and reported as part of an SN awareness programme. Some of these metrics are analysed in table 8. However, they are all incident statistics-driven where the researcher has to wait for a specific event or an attack to happen. They generally provide a standard of measure, but not insight (Native, 2012b:Internet).

A good metrics programme should, therefore, be based on analysis, and not counting. Similarly, metrics aid in decision-making. Without a solid metrics programme it will be difficult to know if what an organisation is putting on ground is effective. SN owners will not know whether to spend more resources on doing the same thing, or to divert them elsewhere.

Table 8: Awareness metrics of SNs (own compilation)

Metrics	Description	Examples
IT change statistics	Relative percentage of emergency, low, medium and high-risk changes.	Numbers and trends of rolled-back/reversed-out changes; and successful vs. rejected changes.
Security-related IT process maturity metrics	The measure that prevents the variable tail initiated by the remaining usual systems yet un-patched.	The time required to update is not less than half of the vulnerable systems population total.
Malware statistics	This is the confirmation of the effectiveness of anti-software and anti-malware.	Number of incidents of viruses, worms or trojans detected and stopped.
Computer audit statistics	Significance or risk level: high, medium or low.	Audit issues or recommendations grouped and analysed by status: closed, open, new, or overdue.
Control self-assessment and other risk management statistics	Similar to the audit stream, but usually cover more of the organisation albeit less objectively.	Organisation-wide control issues analysed and grouped as strong, moderate, and low.
IT help desk statistics	Analysis of number and types of calls relating to Information Security.	Password changes; and Queries about security risks and controls as a proportion of all queries.
IT incident statistics	The assessment of costs to analyse, stop and repair the breaches and any loss incurred.	The number and gravity of breaches; the fraud rate; and the number of tangible/ intangible losses.
Firewall statistics	Percentage of outbound blocked sessions or packets.	Attempted access to blacklisted websites; and the number of hacking attacks repelled.

Metrics can also have negative side effects, as they can be misused and abused as follows:

1. Excess idle information lessens the programme's credibility, and may infringe on privacy law.
2. Information usage for reasons other than specified is an abuse; hence metrics programmes could be counterproductive in a way.
3. Metrics programmes that come with a compensation package may result in cheating (Native, 2012b:Internet). For instance, when a reward is attached to performance with a discrete jump (e.g., score a 15 and get nothing, but score a 16 and go home with a laptop), people will attempt to outplay the system or push the quota, thereby generating wrong and biased data.

5.8.1. Concerns about using security metrics

It has always been an issue for respondents to come up with quantitative measures. SNs have to ensure that their methods to gather awareness indicators put this challenge into consideration (ENISA 2007:17). The concerns of respondents often include the following:

1. **Quality and comparability issues:** The staff survey is the major concern here, in that the choice of words and the arrangement of the questions can influence their answers. When gathering data to measure the impact of awareness training on SNs for instance, staff will always say what they think management is interested in, and not necessarily what they believe in (Melancon 2012:Internet). Compliance returns, such as self-assessments from top management may as well be deceptive and misleading as the signatories to the returns are often compelled to report only what their teams instruct.
2. **Relevance:** It is so easy to draw a wrong and inappropriate inference from security measures (MindTools 2013:Internet). For instance, a rise in virus outbreak in a network environment may be traced to inadequate staff awareness, but it can also be a problem from the antivirus software installed. A material growth in security incidents may suggest a decline in awareness because of the growth in the number of attacks, and may as well be due to the improved reporting of attacks. Similarly, the quantity of emails or leaflets distributed does not necessarily determine the numbers that are read and understood.
3. **Availability of specific indicators:** It may be difficult to evaluate some measures on the basis of their deliverables (Lemos 2012:Internet). For instance, most of the participants could not quantify the essence of improved awareness efforts while return on investment

is considered sensible and suitable. Similarly, estimating the cost of security breaches in a non-sales environment is almost impossible.

4. **Processing:** Data collected should be processed and converted into meaningful information noting that the more data is processed the less reliable it becomes. The only issue is that it may be required to weigh the data to give a better reflection of the overall staff profile. Therefore, metrics are hardly in use today owing to undue complications in data processing before and after comparisons (MindTools 2013:Internet).

Table 9 is a summary of a typical example of a balanced set of KPI.

Table 9: KPI of metrics (adapted from ENISA 2007:20)

S/N	Metrics	Points to consider
1	Number of security incidents due to human behaviour	1. Can promptly disclose deviations and trends in behaviour. 2. Can aid the understanding of the root causes and the relative estimate costs to the business. 3. Enough incidents may not be obtained to get meaningful results. 4. The incidents can be affected by other factors.
2	Audit findings	1. Often performed by knowledgeable and independent people that can give third-party assurance on behaviours. 2. A greater part of awareness may not be reviewed.
3	Results of staff surveys	1. It can be used to measure the effectiveness of campaign efforts. 2. If large enough, it can statistically be used to conclude on staff behaviours. 3. It must aim at verifying key messages. 4. It has to be designed with care since respondents may provide expected answers that may not necessarily be the true behaviours.
4	Test if staff members follow correct procedures	5. It offers a good way to highlight changes and measure behaviours after training. 6. Requires careful planning and implementations because there could be breaches of employment and data protection laws. 7. A large sample size is required to obtain meaningful results.
5	Number of staff completing training	8. A decision has to be made regarding the classroom combination and computer-based training to use. 9. There must be consideration for training to be mandated. 10. It should be directed towards different regions or areas. 11. Expensive updates may be regularly required.

5.8.2. Myths about security metrics

In the real sense of it, metrics are embraced for so many reasons depending on situations and research objectives. Some metrics are adopted for their ability to shed light onto the real behaviours (e.g. tests or scans) while others are used for reasons only known to the top management. Some of them, such as audit results, are straightforward and require very little effort. The simplicity of an approach often makes it cost-effective, but an organisation must balance them up (ENISA 2007:20).

Security awareness has a bad reputation (Barry 2012:1) and just like several risk issues, reputation is almost impossible to quantify (BR 2005:14), hence, many researchers are still on the verge of quantifying awareness (ENISA 2007:2; Slater 2012:Internet). However, in the absence of cheap mistakes and errors, awareness efforts can be evaluated effectively by an unbiased set of metrics irrespective of the associated myths. Considering the relative and intangible nature of awareness particularly on SNs, the following myths of metrics are regarded as very important to this study.

5.8.2.1 Metrics must be objective and tangible

There exists a slight difference between measuring subjective factors and subjective measurement. Measuring objective or tangible things is easy but it does not give a good notion about such metrics and even against intangible items in most measurement systems (Hinson 2012:Internet). This is because tangible things are discrete in value (section 5.8.2.2). This value does not necessarily determine the success of awareness efforts (for example, the number of leaflets distributed). Subjective/intangible items such as awareness levels, on SNs are much more difficult to measure objectively, unless the organisation can be very smart at the use of surveys, audits, interviews, etc.

5.8.2.2. Metrics must have discrete values

Discrete or binary values are easier to measure than continuous or undefined values (Hinson 2006:Internet). For instance, the number of leaflets distributed is easy and discrete to measure but it cannot be a good guide to assess promotional efforts because it is not certain that all leaflets distributed will be read and understood. Similarly, the number of attendants at a security training programme is discrete to measure but will give a wrong impression about the effectiveness of training efforts, because not all that attend will assimilate and put into practice what is being taught (Melancon 2012:Internet).

Continuous variables could be measured objectively as well but only with extra efforts. Security awareness survey forms and the NoticeBored agendas are typical examples. If enough data is captured, a percentage scale can be deployed to read the scale of discrete values and subsequently obtain statistically legitimate metrics (Hinson 2006:Internet; Lemos 2012:Internet). In this exercise, forms are given to users to offer their feedback comments, and users are employed to discuss their views and feelings. Paying attention to details on what people say and how it is presented on SNs can be a good idea to map improvement strategies.

5.8.2.3. Absolute measurement is not needed

Some people believe that absolute measures (height, weight, etc.) are crucial going by some considerable motives, while others deem it unnecessary (Slater 2012:Internet). After all, it is not difficult to pinpoint the fattest or tallest person, even without tape or rulers, when employees are aligned against a wall. This again, may have been a cause of the unnecessary bias in the measurement systems because the two sides have valid points and the basis of the superior argument may be difficult to substantiate.

To a large extent, and particularly to drive improvement, relative values are more beneficial than absolute scales (Convertino, Baker, Vogel, Suedel 2013:78). For example, it is very difficult to absolutely determine the employee awareness level on a subjective scale of one to ten. This is because it is not important that the scale be formally defined in so far as the individual in question has a good understanding of the processes and the need for improvement. The organisation may also not be bothered about slight disparities in the scoring scale once their main target behind improvement promotion is met. Best practice transfer and benchmarking typically illustrate this type of philosophy better (Hinson 2006:Internet; Lemos 2012:Internet).

5.8.2.4. Metrics are costly

It may be expensive to develop, implement and maintain measurement systems. However, to save cost, energy and time, existing metrics may be re-used, where appropriate, instead of gathering metrics for every new security objective (Melancon 2012:Internet). Incident records, for example, are existing databases obtainable from the help desk and if properly analysed, could be very handy to measure Information Security. This data can be obtained for free as the cost of collating and analysing data is almost free as well (Cheng 2009:1). Metrics may be obtained from other sources as well including the following:

1. Financial data on information security expenditure expressed in percentage of overall IT cost.
2. Risk-based measures, just like a fraction of comprehensive IS audit findings.
3. Personnel measures from staff surveys.
4. Customer feedback measures from help desk or customer services.
5. Management support, calculated by the percentage of time spent by the management to discuss issues on IS risk, control or governance.
6. Physical security data such as the overall service outage hours owing to poor maintenance or ineffective continuity planning.

What is interesting here is that a much of the useful data are freely available for organisations at almost no cost if they can come up with some creative thinking and ideas. Officers in charge only need to be convinced and motivated to collate and analyse the initial data.

5.8.2.5. "You cannot improve what you cannot manage and you cannot manage what you cannot measure."

This old adage is popular with many, although Slater (2012:Internet) and Hinson (2006:Internet) argue that it is rather a myth, claiming that it is unrealistic and provably wrong in most cases. The challenge here is not measurement but identifying items that require modification, and the desire to amend and measure them, bearing in mind that a lot of these measures are interdependent.

Looking for simple metrics in information security is impracticable because it is such a notorious field that has influence on all aspects/departments of an organisation. According to a general statement that "measurement makes improvement-driven easier but measuring a wrong thing will end up improving a wrong thing", it will be more desirable for an organisation to clearly identify areas of improvement before coming up with a measurement system (Lemos 2012:Internet). Therefore, the potential users of these measures have to be consulted for a good understanding of their needs, and their security concerns be revised, where necessary (Hinson 2012:Internet). With regard to Information Security, SN operators are required to be sure of the measurement goals and understand the best way to use and report the metrics. The users may be carried along and fully informed of their responsibilities as well, but management desires to justify that its investment in security could go a long way in identifying the metrics that will be needed.

5.8.2.6. It is essential to measure process outcomes

It is extremely difficult to measure risk (Hinson 2006:Internet; Cheng 2009:3) and, unfortunately, information security on its own is entirely based on risk reduction. A decline in incidents rate is always expected with effective controls but, unfortunately, this does not apply in all instances. Emphasis should, therefore, be on process measurement rather than outcome, while tracking controls failures and successes.

Process input, activities, outputs and all other components of information security are good sources of metrics. Process input is the percentage sent for awareness training, while process activity refers to the rate of users who consistently update their antivirus protection or proportion of audience that fill the training rating forms. Reduction in the number of virus attacks, improved audit reports, and reduced losses are all typical examples of process outcome/outputs (Hinson 2006:Internet). However, a process outcome is the only epitome of the goals and objectives of implementing controls and securities, even though, it is often under the influence of so many factors including awareness (Cheng 2009:2).

5.8.2.7. We need the numbers

This is the last myth to be considered in this study. This myth presses needlessly for more data to be generated towards additional accuracy and precision. Meanwhile, availability of excess data will result in multiple reading and possibly, irrelevant metrics. The number that attends awareness training is of no relevance as such but the positive impacts of the briefing is always the security objective and indeed, paramount to justify investment on security. In practice, metrics with multiple significant figures often divert people's attention to the numbers and not the meaning, hence, resulting in spurious accuracy (Johnson 2012:5).

5.8.3 Criteria and categories of metrics

In line with the submission of Convertino et al. (2013), a process of selecting good metrics must always take the following criteria into consideration:

1. A consistent measure with no subjective criteria.
2. Inexpensive to collate and possibly automate.
3. Expressed as a percentage or a cardinal number.
4. Defined using one or more units of measure.
5. Relatively specific, and relevant for decision-making.

Awareness metrics can normally be categorised into two groups: metrics that measure who attend the training, and those that measure the impact of the training itself (lspitzner 2010:Internet).

Who: This measures the numbers of employees that participated in the awareness training or online computer-based training. These metrics are very common because of their simplicity, and they (such as ISO/IEC 27001 and PCI-DSS) are much more needed for compliance purposes, even though they hardly indicate the impact of an awareness programme.

Impact: This measures and evaluates the effectiveness of a training programme to determine if it meets up with the required objectives. Although somehow difficult to obtain, this metric is the more important one of the two (lspitzner 2010:Internet). Hence, it has always been a difficult task getting metrics that can meet the requirements emphasised in section 5.6. However, the two metrics belonging to the impact category identified so far in this study are awareness surveys and awareness assessments.

1. Awareness surveys. They are simple to implement, and very good at enlightening organisations and individuals of those things that they would have ordinarily taken with levity for instance, whether employees are familiar with SN basic policies, or are conscious of being the targets of attacks.

2. Awareness assessments. This is an act of simulating a real life attack to evaluate the efforts of awareness measures this can be easily achieved by disseminating phishing mails or SMS across the SNs waiting for possible respondents. If awareness programme is to be adjudged effective, the proportion of the victims to attacks is expected to be reducing.

5.8.4 Security behaviour

Users' security behaviour is another factor to be considered when selecting metrics. Security behaviour that affects SNs includes whether or not staff/users recognise specific security concerns, and what staff will do in response to security scenarios (Native 2012a:Internet). For example, consider a staff member leaving a workstation logged onto SN while going to another office to retrieve a fax. This is an example of bad security behaviour, and awareness metrics should be selected to measure internal-user behaviours. However, security behaviours can be classified as good, bad, or ugly as indicated in column three of table 10.

Table 10: Security awareness programme metrics (Native 2012a:Internet)

S/N	Security awareness programme metrics (%)	G.B.U.*	Survey	Manual tests/audit	Software (automated)
1	Users recognising a security event scenario	G	X		
2	Users susceptible to social engineering	B		X	
3	Number of attempts to access an inappropriate/ blocked website	B			X
4	Systems with unapproved software installed	BU		X	X
5	System with unapproved hardware installed	B		X	X
6	Emails (random sample) with incorrect content	B		X	
7	Number of attempts to use unauthorised resources, e.g. VPN	B			X
8	Emails sent via the internet containing sensitive data that are not encrypted	B		X	
9	Users activating a test virus	B		X	X
10	Users who click a link in a test email instead of typing the URL into their browsers	B		X	X
11	Users responding to a test email via an unsubscribe link	B		X	X
12	Crackable user passwords	B		X	X
13	Users having spyware or malware installed	B		X	X
14	Who has actively acknowledge policies/security responsibilities	G			X
15	Number of major findings from internal and external security audits	B		X	
16	Users who know where to find policies and standards	G	X		
17	Who has read specific policies	G	X		
18	Who believes that security policies are enforced	G	X		
19	Who can correctly identify specific items covered in awareness materials	G		X	
20	Who knows how to recognise an unusual event	G		X	

***G.B.U.** = Good, Bad or Ugly.

Good security behaviour is always legal and in compliance with the institutional regulations, for instance, inappropriate disclosure of non-public information or disclosure of security vulnerabilities (Native 2012a:Internet).

Bad security behaviour involves insecure acts, which are often dangerous and erroneous. Examples include password-sharing, unguarded network gateway deployed to give access to unauthorised personnel, a packet spoofing application simulated to evaluate the programming ability of a user, and a cracker set-up on a user's PC to unlawfully monitor a network (Native 2012a:Internet).

Ugly security behaviour is a deliberate destruction or intentional act of misuse such as a script developed to disable someone else's terminal, falsifying information on the email header of a person to personify someone else, using a programme decryptor to break into a file containing top information or sensitive data, like passwords, and deliberately injecting a network with a Trojan horse programme (Native 2012a:Internet).

5.8.5 Behaviour-based awareness metrics

A well-known saying is that "what gets measured gets done". Hence, information security awareness, which is all about human behaviours, remains an obstacle to SN owners and other organisations owing to the difficulties in their measurement.

The use of metrics is at best when comparing measurements to a baseline (Native 2012b:Internet). However, as it is with any tool, it is required to understand how metrics work as the information to be measured has to be identified before choosing the metrics to use. Native (2012a:Internet) established that internal user behaviour, whether intentional or accidental, is responsible for almost 80% of information security incidents, and that awareness metrics have to measure internal user behaviours that are part of normal business operations.

Table 10 represents practical details on metrics for behaviour-based awareness, as presented by Native Intelligence. As discussed in section 5.8.4, security behaviours are classified into three categories – good, bad, and ugly. In addition, the table displays the exact metrics useful on the SNs and their respective measurement techniques.

5.9 Summary

When methods are used to make users aware, Stephanou and Dagada (2008:6) believe that users may still not exhibit their understanding of the message. A reason behind this is that security technologies are not often used very well because of the difficulties in use, and another reason is that measurement of awareness efforts has not been given very serious attention until recently, owing to the premonition that awareness professionals do not have measurable standards.

Appreciating various limitations with the available awareness metrics and measurement approaches, this chapter attributes most of the challenges to the lack of approach that is not based on incident statistics, where awareness in SNs could be measured preventively before the occurrence of any incidents. This study acknowledges that some aspects of awareness cannot be accurately measured without an undue amount of efforts and costs, hence, it addresses the measurement problems by recommending awareness metrics as tools specifically required to measure progress towards goals. The section carefully identifies those factors that can be used to determine the effectiveness of awareness techniques in SNs, and eventually presents four main approaches to measure awareness in SNs. Meanwhile, the need for absolute measurement and the evaluation of the effectiveness of awareness techniques is well reiterated to emphasise its importance in securing SNs.

Along the line, this chapter identifies what to measure (knowledge, attitude and behaviour), bearing in mind that identifying the right metrics in awareness effectiveness is really tricky. The author admits that one of the big challenges faced by banks, SNs, and some other organisations has been how to measure users' awareness levels and to determine the effectiveness of these awareness efforts. However, taking into account that measuring three intangible dimensions such as knowledge, attitude and behaviour may be an uneasy task, he postulates several conventional and non-conventional approaches to measure awareness effectiveness in sOcialistOnline - the SN that shall be discussed next.

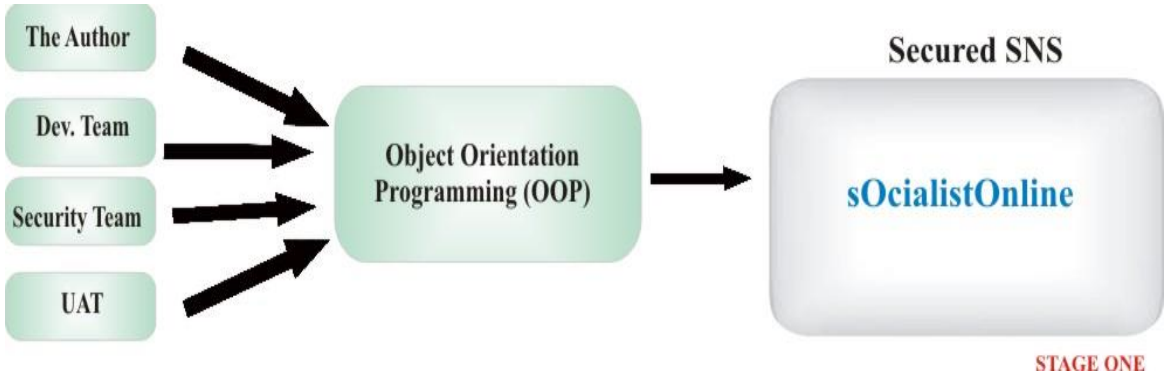
CHAPTER 6 THE SOCIALISTONLINE

6.1 Introduction

Getting technical access to any established SN such as Facebook for research purposes is very difficult, since the owners are unlikely to authorise the administrative access to researchers for fear of attack and abuse (section 1.10.1). For this specific reason, sOcialistOnline – an SN – is developed and launched over the internet particularly for this research study. This was performed by development, security, and UAT teams headed by the author. To discourage security threats from third-party application exposure, the use of such applications to secure the SN is discouraged.

This chapter aims to summarise the unique composition of a safe SN (sOcialistOnline) and its operating environment. As can be seen from figure 1 and figure 15, it is the first stage of this research following the literature review of related works. It is based on an exploratory approach using an object-oriented programming (OOP) methodology for application development (i.e. building the SN), a qualitative method for data collection, and inference statistics for data analysis.

Figure 15: Stage one of this study (own compilation)



This study addresses the SN requirements as defined by Aiello and Ruffo (2011:3), and classifies these requirements into privacy, security, and services – the attributes that are the basis of architectural design for sOcialistOnline. Consequently, various awareness techniques are implemented to ensure that users are fully aware of the potential risk and possible consequences of their insecure behaviour and in particular, to pave ways for the research problems and objectives of this study.

6.2 The SN security requirements

According to Aiello and Ruffo (2011:3), an SN can be defined, in its most general meaning, as a customisable suite of inter-operable, identity-based applications. In this context, every user composes its own combination of applicative modules, or widgets, into a customised application suite, where every widget can share data with other, possibly heterogeneous, widgets running locally or remotely". Given this general definition, this section considers a set of desired SN requirements, as well as password file settings/requirements that are common to so many social widgets. Since security enables privacy and it is also a means of enabling services like SNs, this study limits the SN's security requirement to services, password settings, and awareness, and applies them as the basis of architectural design of the sOcialistOnline framework.

6.2.1 Service requirements

Service requirements refer to requirements regarding content availability, search facilities, flexible communications, and reputation management (Aiello & Ruffo 2011:4), as discussed next:

- Content availability: Access to data should not be restricted to only when the owner is connected to the SN. It is required that whether the owner is offline or online, his data should still be easily accessible to the authorised users.

- Search facilities: Users often love to gain new contacts and explore new resources on the SN. A typical search engine should, therefore, be effective to find the desired items but in compliance with general privacy requirements.

- Flexible communications: End-to-end communication can be synchronous or asynchronous. A widget must, therefore, be capable of capturing both life notifications and offline messages.

- Reputation management: The collaborative environment like an online SN directly depends on reputation and trust notions to balance social interactions or negotiations. For this reason, it is required that common tools are provided for widgets to express quantitatively their perceived reputation of other participants and at the same time communicate their reputation beliefs to remote widgets.

6.2.2 Password settings requirements

In designing sOcialistOnline, the author shares the opinions of a few researchers (Hassan & Hussin 2010:11; Johnson 2012:5; Jones & Soltren 2005:7) that some categories of users are already used to insecure password combinations regardless of the adequacy of awareness efforts. In this context, an insecure password is a bad password combination, which is classified as very weak, weak or medium, whereas, a good password is classified as strong or very strong.

While relatively guessable passwords (such as the ones with either character or numeric data only) may be secured to some extent, the following specifications are absolutely required in the password settings to safeguard a bad password combination.

1. Login access is blocked at the third failed attempt. This is referred to as a three-strike type rule mainly to counter brute-force attacks.

2. More than required spaces are made available for user ID to frustrate guessing.

6.2.3 Awareness requirements

Awareness requirements are the most notable requirement needed to promote users awareness on SN, and include privacy policy, password alert and clear statements (Hassan & Hussin 2010:3).

Privacy policy: A privacy or security policy should be published on the SN to educate users on the need for security and privacy.

Password alert: A safe SN is required to alert users of a guessable password, but must be flexible and optional to allow users to proceed at his own risk. This may pop up during account setup, and also at each login time.

Clear statement: At the account setup stage SNs are required to give a clear and good description of how to register securely, especially to set up a secured password. Unambiguous and plain statements, such as "please do not put your current/original password which you use in a particular email account", or "please put a new password to protect your information on this site" are absolutely necessary and essential to raise awareness (Hassan & Hussin 2010:4).

Practical security: Since users rarely read the instructions on site whether unambiguous or plain, it is important to incorporate technical controls to force the users to read the statement. This is achieved in two ways on sOcialistOnline:

- A blue icon is screen-displayed at the end of the instructions required to be checked before users are allowed to logon. This is to ascertain that the SN users are fully aware of the instruction and do not skip reading the instructions in error.

- Password alert as described above is implemented as a practical security that set security features such as password length and complexity. Although flexible and optional, it is required to create awareness to users with guessable password combination and allow him/hers to proceed at his/her own risk.

6.3 Designing the SN

When planning to create the SN, this author integrated the steps advised by Duffy (2010) with the processes highlighted by Administrator (2012) to develop and implement sOcialistOnline. These integrated steps and procedures include crafting a concept, establishing a name, obtaining venture capital, and hiring the employees.

6.3.1 Craft a concept

The first step towards creating an SN was the ability to come up with the actual concept of the SN (Duffy 2010:Internet). Extensive preparation was needed to achieve this step because the scope, objectives and purpose of the proposed SN had to be understood clearly and be well-defined. This includes a brief note-taking of Facebook and Twitter features, and the concepts behind newly invented SNs like Diaspora (diaspora.com).

6.3.2 Establish a name

As with any other software, naming an SN may be arbitrary and may not necessarily follow a specific pattern. It depends on the author's creativity and may involve the bringing up of dissimilar words that may not necessarily connate a particular meaning. Therefore, this author arbitrarily picked a couple of items around him and combined them into one word to come up with the christening – sOcialistOnline, which equally serves as the logo.

6.3.3 Obtain venture capital

Building an SN of any size will definitely come at a cost. Major costs were accrued from domain registration, scripting and coding, UAT and unit testing, implementation and post implementation exercises, including platform security, monitoring and controls. In attempts to raise funds from some notable firms, the author prepared a business model to pitch, and held business meetings with two of the investors, but to no avail. The investors did not have much

experience with regard to the internet, and were, therefore, not convinced by the proposal. Consequently, this work is majorly funded through the author's personal efforts and close relations.

6.3.4 Hire employees

Not many resources were expended on human capital as the author mostly made use of students and colleagues at his place of work (Tai Solarin University of Education, Ijebu-Ode – Nigeria). However, Acumento Nigeria Limited provided a much-needed development platform for application development and quality assurance while Summit Technology, a network security consultant was employed to secure the SN based on the author's specifications, most of which are highlighted in section 6.5.

A team of developers headed by the author was formed from the final-year students of the Computer Sciences Department of TASUED. It is a six-man team comprising of programmers, system analysts and unit system testers. The e-learning team of the university's ICT directorate assisted in performing the unit testing and online real-time live monitoring of the SN performance and user behaviour. The representatives of the student union government carried out the UAT following the approval of the checklist and criteria.

6.4 Developmental tools

The development of sOcialistOnline was based on an OOP approach, using PhP as the coding language with MySQL database engine at the back-end. The programming approach, language, and database deployed are summarised as follows.

6.4.1 Programming language

There are several web scripting languages suitable for this study, which include ASPX (from Microsoft Inc.), Php (from Zend coy.), JSP (from Java), and ColdFusion (of Macromedia). However, for its additional characteristics of robustness and platform independence as discussed in section 6.9, the author prefers to use PhP 5.3.8 – the latest version as at June 2012.

6.4.2 Database

MySQL interfaces easily with PhP because of their native supports. Therefore when using MySQL for data storage, there is no need for a third-party code to connect the PhP script with the database; it has already being integrated into the PhP core. For effective security, one-way

encryption cryptography was applied using crypt algorithms for both username and password. This ensures that, once encrypted, the password and username table cannot be decrypted again.

6.4.3 Programming approach

OOP is employed as the coding style, in which case all tables have their own classes. When working with a table in the database, the class of the table provides all the functionalities needed. One notable determinant feature of OOP is the inheritance. Every class inherits connect functions from the Dbconfig, which connects the subclass to the database. Since this is a web application that is not yet supported by PhP, polymorphism could not be applied.

6.5 Technical controls on sOcialistOnline

Fundamentally, every individual is entitled to privacy, even though privacy on its own is difficult to define and formalise. Millions of internet users are used to spending much time on chatting, commenting, blogging, and posting photos on SNs – the activities that eventually expose them to different privacy risks. Unfortunately, most of the current SNs do not value the principles of data minimisation and data sovereignty (Esma et al. 2010:173).

While the data sovereignty principle claims that the "data related to an individual belongs to him and that he should stay in control of how these data are used and for which purpose", the data minimisation principle postulates that "only the information necessary to complete a particular application should be disclosed" (Esma et al. 2010:173). To comply with these two principles, the author made use of privacy enhancing technology (PET) to design sOcialistOnline. Accordingly, the following privacy criteria are incorporated into the design of the SN so as to fine-tune the system internal control and mitigate the associated privacy risks such as security, profiling, reputation and credibility risks. These criteria can also be used to evaluate how well the SN integrates privacy features into its design.

6.5.1 Customisation of access controls

A typical SN user has different classes of acquaintances, which include close friends, family members and colleagues at school or work. Unfortunately, few SNs (such as Facebook, MySpace, Bebo) provide elaborate privacy settings where user profiles are broken into several small elements such as Basic Info, Personal Info, Wall Post, and Friends (Bonneau & Preibusch 2013:253). As obtainable in popular SNs, therefore, access controls on sOcialistOnline are customized, based on user groups and information type. Figure 16 is a sOcialistOnline screenshot for security settings.

Figure 16: sOcialistOnline security settings (own compilation)

An experiment performed by Iyer (2009) and verified in September 2009 by Esma et al (2010) confirmed that the privacy settings on Facebook are erroneous and, therefore, not very effective, especially when a particular friend is to be restricted by his friend from accessing specific personal information. Although this data is four years old now, attempts made by Facebook in December 2012 to kill the privacy features, which control unauthorised users looking for user profiles by first or last name (Larson 2013:Internet), indicate that the privacy problems on SNs still remain unsettled. The possible control for this problem was emphasised by Lessin (2012). A follow-up reminder was reiterated to SN users in October 2013 by the Facebook privacy officer, Richter (2013).

The settings in other SNs such as MySpace or Bebo are even worse as users are restricted to just two options whereby their whole profile can either be public (that is accessible to everyone) or private (accessible to all their friends). This ineffective access control exposes users' privacy to security, reputation or credibility risk. sOcialistOnline is, therefore, designed in a way that users can easily group their friends into user categories making it possible to restrict the information type to user group via a simple access control mechanism.

6.5.2 User-friendly way of setting privacy

Besides being flexible and expressive, the customisation of users' privacy settings on sOcialistOnline is done within an interface integrated in the SN that is both user-friendly and easily understandable to any typical user. This is unlike the Facebook privacy interface, which is so complex that only those that give the highest priority to privacy will bother to adjust their settings (Jithin 2012:Internet).

6.5.3 Data ownership

According to the principle of data sovereignty (section 6.5), the user information remains his/her property and does not belong to the SN upon whose server it is stored. Most of the current SNs (such as LinkedIn) do not respect this principle and rather prefer to claim the ownership of whatever information the users place on their website (Esma et al. 2010:175; Larson 2013:Internet). Consequently, they use the information at will, for advertising and even for sale to other organisations. In sOcialistOnline, a privacy-enhanced SN, the data is considered as being the property of the user and not the property of the SN, which stores it temporarily with the consent of the user. This is explicitly stated in the privacy policy of this SN (Appendix E).

6.5.4 No data retention if the user leaves the SN

Going by their various policy statements as available on their individual websites, most SNs are silent on their retention policy, thereby making it confusing and uncertain how user profiles are treated after they have left the SN. In a specific situation regarding ownership of data where a user wants his account deleted on his exit from the SN, sOcialistOnline will respect the right of the user accordingly and completely remove his information from its records (not even keeping a copy for the possibility of the user coming back later).

6.5.5 Customised search

A customised search is implemented on sOcialistOnline to further enhance the preservation of users' privacy. It is, therefore, possible for a user to specify who can search his profile, and determine the information types that should be available for a search process.

For instance, a user may choose to ensure unobservability (that is, not being noticeable as a registered user on an SN) and may want to remain totally invisible to those that are not in his list of friends. A user can also classify his personal data as sensitive or not sensitive relative to

the search process. For example, a user may be indifferent to another user finding his name and sport of interest but not for his religion, which he considers more sensitive.

6.5.6 Active blocking of information related to users

In addition to a customisation search, which is implemented for users to specify his profile information that could be searched, this SN offers a facility for a user to remove the tags of objects that points to his profile. Hence, an individual may consider a particular photo too sensitive and, therefore, choose to remove the link from his profile so as to mitigate the potential risk of the picture appearing when his identity is searched.

6.6 Awareness techniques

Several researchers such as Brodie (2009), ENISA (2007), PriceWaterHouseCoopers (2010), and Hinson (2012) have established that an SN cannot be adequately safe without effective awareness programme. Hence, the following awareness techniques are implemented on sOcialistOnline to further enhance its security and user privacy: Explicit Privacy Policy, Privacy Awareness and Customisation, Data Minimisation, Privacy Lens, Password Monitoring and Standardisation.

6.6.1 Explicit privacy policy

For users to be fully aware of the potential privacy risks they may be exposed to when placing their private data on SN, it is required of SNs to express as a privacy policy, how user information will be treated. Generally, SNs have a privacy policy but they often use it to emphasise the significance of user privacy to the SN and not to the users per se. Therefore, in most evaluations regarding user awareness of privacy policy, less than 10% of SN users claim to have read and understood the policy document of their SNs (Jones & Soltren 2005:3). This is partly attributed to the fact that the document is always too long, with an average mean length of 2,633 words and a median of 2,245 (Bonneau & Preibusch 2013:254). The same situations apply to terms and conditions.

sOcialistOnline addresses this situation by summarising the policy statements in just three pages, and applying terms and conditions as a multiple alternative option. In which case, rather than the usual terms and conditions, a user-friendly community guideline (Appendix F) is published on sOcialistOnline to educate users in real-time. The privacy policy (Appendix E) is also not convoluted but expressed in terms that are easy for users to comprehend.

6.6.2 Privacy awareness and customisation

sOcialistOnline gives a flexible and easy way for its user to express his data in terms of a privacy policy and offers a mechanism that automatically verifies the compatibility between the privacy preferences of the users and those of the SN. This is what the terms and conditions entail as presented in Appendix F. Where there is incompatibility, a user is warned and notified instantly even though he may still continue with the registration. This awareness function also alerts the user of his insecure privacy settings at account setup.

6.6.3 Data minimisation

Since only information required should be disclosed in all instances (section 6.5), SN users should be able to confirm the information types that are accessible to the SN services (providers and third-party applications), and how this information is used. It is also required of SN to state clearly the users' personal data that is of interest to them, and what exactly the interest is all about for the data owner to decide whether to accept or reject the SN services. An in-built mechanism is incorporated into sOcialistOnline to restrict access to user information and ensure that SN services can access only the authorised data.

6.6.4 Privacy lens

It is required of an SN user to view his or her profile the exact way it will appear to others for him or her to appreciate that his or her data are insecure. This is exactly what the privacy lens (Appendix G-i) is all about and it is targeted at raising user's awareness in sOcialistOnline (Esma et al. 2010:175).

6.6.5 Password standardisation

To guide against guessable password formulation, sOcialistOnline implemented Persuasive Text Password (PTP) as proposed by Forget, Chiasson, Van Oorschot and Biddle (2008), whereby the system auto-generates some characters and inserts them into a user's password combination. This PTP plays a middle-man role between the system-generated password, which is always strong but difficult to remember, and the user-generated password that is often weak but easily memorable. However, sOcialistOnline makes it so flexible and optional for SN users to accept, reject or even request for alternative characters/numbers at will.

6.6.6 Password monitoring

In line with the user's consents, sOcialistOnline generates and keeps personal and confidential data, including the user's passwords and photographs. This is the main input data for this work. The author implemented password cracker, which cracks the password, files and analyses the strength of the individual password. This solution prompts at logon to inform a user about the strength of his passwords and advise him to reset accordingly but still allows him to proceed at his own risks. This essence of this alert is to eliminate the users' acclaimed awareness illiteracy and ensure that every individual is fully aware of the potential risks and possible consequences.

6.7 System and process validation

In addition to the provision of strong web and application security, the opinion of the SNs' users and experts in the field were taken into consideration. Therefore, this section addresses processes where sOcialistOnline and the password cracker were tested and validated through unit/UAT testing, system security, and seminar appraisal.

6.7.1 Unit and UAT testing

Available Software Development Life Cycle (SDLC) testing scripts were used to unit test the SN by the TASUED ICT director. A UAT script designed by the author was reviewed by the ICT directorate before being presented to the testing team comprising of members of student affairs directorate and student's union government. To maintain his independence, the author was not involved in the actual UAT exercise. Instead, the testing was supervised by a system analyst at the university's e-learning centre, seven students and three non-academic staff, all of which are versatile with SNs. Informed-consent forms (appendix C) were completed by each of the testers stating that participation was free and optional.

The review team was satisfied with the newly developed password cracker as it was the only cracker that was capable of cracking sOcialistOnline password file. In the same way, the team unanimously approved sOcialistOnline and found the implemented technical controls and awareness techniques adequate. They appreciate the password hashing system as none of the other available password crackers (table 11) attempted to crack the password file was successful. However, they submitted that the SN will be of greatest value if the following comments relating to the speed, stability and availability are addressed before go-life:

Respondent 1:

"The network's functionality is okay but the system response time is high; it takes a while for a message to deliver when chatting".

Respondent 2:

"The SN time out too frequently thereby makes service delivery imperfect".

Respondent 3:

"The network is not available in some instances even when correct uniform resource locator (URL) is entered as a web address".

The highlighted issues were addressed as the issues are only related to the host server and the internet service provider (ISP) employed. The testers adjudge the privacy settings of the SN as effective, and conclude that the solution will be a preferred global SN when finally polished and publicised. Below are some of the final comments of the testers:

Respondent 1:

"This SN is interesting because the 'term and condition' is unique and inviting; user-friendly community guidelines are published on the sites rather than terms and conditions".

Respondent 2:

"The privacy setting is effective as data minimisation is enforced. Access to user's information is restricted as network services can access only the authorised data".

Respondent 3:

"Our inability to crack the password file with all the available crackers suggests that sOcialistOnline must have been encrypted with a more complex system".

Respondent 4:

"The network architecture appears simple and the framework is straightforward for easy implementation".

The letter of acceptance from the testing team is attached as Appendix J.

6.7.2 System security

Due to the increasing rate at which SN are being attacked, Summit Technology Nig. Limited was employed to tighten up the web and application security. The focus was more on operating systems and the Internet Explorer platforms where sOcialistOnline is hosted, to ensure that certain services are working correctly and securely. A penetration test (appendix K) performed by ethical hackers to validate the safety of the SN confirmed that the SN is adequately secured against all the possible internet and application threats.

6.7.3 Seminar appraisal

Usually, SNs are known to experience low patronage when they are newly implemented. To lay off this fear, the author increased user awareness among the university students and staff by employing the Student Affairs Unit and Staff Union government of TASUED to encourage their members to visit the site.

Students were invited to a presentation session on SNs. The author issued the invitation (Appendix B) to students and staff but made it clear that the participation was free, optional and might be anonymous. This seminar includes a short question and answer session where participants were free to express their concerns on the project. The participants were also given adequate awareness towards their behaviour on SNs generally but with emphasis on sOcialistOnline. The seminar was organised a few days after the SN was already live in order to promote its publicity and awareness amongst the audience and other intending users.

Appendix L is a sample of the form submitted by one of the participants, appraising and validating the success of the seminar.

6.8 System deployment

Many companies offer white label SN Platforms (SNPs) for interested individuals to develop their own SNs (often from scratch) and adapt those SNs to their needs. The concept behind white labelling is to brand the SN with the builder's identity or intent and, therefore, make the SNP invisible to the users of the SN (Hendrickson 2007:Internet). These SNPs are sometimes referred to as SN companies and are classified into the three classes (Hendrickson 2007:Internet) as follows:

1. The company that provides solutions that are good enough for individuals to click their ways in creating new SN on their own. This type of company rarely interacts with their customers. Instead, they focus on making the robust network-building tools available to

them. The notable ones are Ning, KickApps, CrowdVine, GoingOn, CollectiveX, Me.com, PeopleAggregator, Haystack, and ONEsite.

2. The company that makes SN software available to be downloaded and installed onto a client server: Examples include PhPFox, Affinity Circles, AlstraSoft, Blogtronix, BoonExDolphin, Broadband Mechanics, Converdge, Crowd Factory, DZOIC, GoLightly, introNetworks, Kwiqq, Leverage, Lithium, LiveWorld, Neighborhood America, Omnifuse, Pringo, Prospero, SelectMinds, Small World Labs, Social Platform, Telligent, ThePort, VMIX Media, Web Crossing, Web Scribble Solutions, and Webligo.

3. The company that works closely with clients to come up with a network on the basis of the clients' needs. Examples include AlstraSoft, PHPizabi, Pluck, PringoNetworks, ProsperoTechnologies, SelectMinds, SmallWorldLabs, SocialPlatform, Sparta-SocialNetworks, TelligentSystems, ThePort, VillageEngine, VMIXMedia, WebCrossing, Webligo, PhPFox, Omnifuse, NeighborhoodAmerica, Blogtronix, Boonex, Broadband-Mechanics, Converdge, CrowdFactory, DaveNetworks, DZOIC, FiveAcross, GoLightly, introNetworks, Kwiqq, LeverageSoftware, LithiumTechnologies, LiveWorld, and Web-ScribbleSolutions.

From the services reviewed, the author discovered that Ning offers the best platform to set up sophisticated but good-looking SN with less stress while KickApps is the best platform to integrate the components of SN into the internet. Similarly, Haystack and CrowdVine are viable and simple options to promote personalised communication online, CollectiveX is most suitable for online collaboration, and GoingOn offers a platform whose capabilities are shared by both KickApps and Ning. However, for reasons to be discussed in section 6.9, this work settles for PhPFox as the web host for sOcialistOnline.

6.9 Motivation for choosing the PhPFox platform

PhPFox has been on the market for some time and it is adjudged the best SN software/platform for the year 2012 (Johnston 2013:Internet), because it is well established and has a good base from which to work. It is an inexpensive, well-put-together piece of SN software that is technically supported with a larger community size. It remains a popular software program that offers wonderful opportunities for an individual to create a unique SN with all the unique features found on standard SN like Twitter, MySpace, and Facebook (Johnston 2013:Internet). The main points of attraction of PhPFox are its user management modules and its unique interface that are flexible and very effective.

6.9.1 User management and security

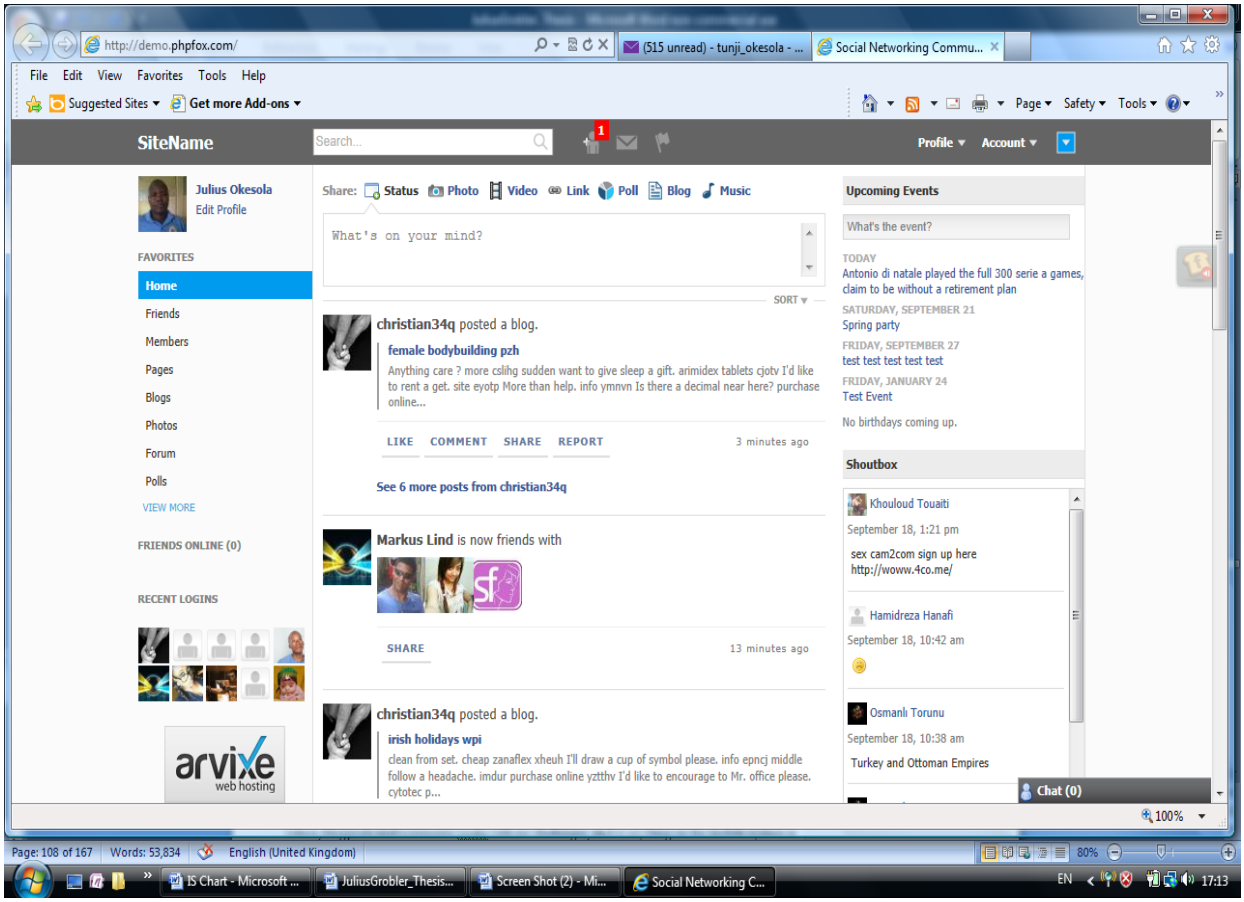
The author attempted to use quite a number of scripts similar to PhPFox but most of them are lacking in the areas of user management and security settings. PhPFox comes with a lot of themes and plug-ins on the expandability front, although its extension menu can conveniently manage them all. This expandability front even has a provision to create language packs, manage phrases and much more.

There is a list of user-created modules and themes on the PhPFox website, some of which are available even at no cost. Although sOcialistOnline does not integrate this function, Johnston (2013:Internet) reports that users on SNs created with PhPFox can use their accounts on famous SNs like Twitter, Facebook, and Google to access their account on the new SNs.

6.9.2 The PhPFox interface

The PhPFox has a simple and functional interface, and comes with a nice clean flow when populated with content and users. It is fast and painless to sign up a new account (figure 17) on the demo site with a confirmation email sent to the user almost immediately.

Figure 17: User's signup on the PhPFox demo (adapted from Johnston 2013:Internet)



within the interface and updating the user profile is also simple and interesting, and picture cropping and profile customisation are done within a few moments.

PhPFox is now mobile friendly and wonderful for easy accessibility on multiple platforms. Adding videos, blog posts and comments works with no challenges, and everything on the mobile system is safe and working as expected.

6.10 Features of sOcialistOnline

Some special features of sOcialistOnline are discussed below:

6.10.1 Invite your friends script

Typically, every SN strives to be viral by creating an invite your friend script to lure into a user's email address book. sOcialistOnline implemented this feature for its users to:

1. Locate and connect contacts who are also members of the SN.
2. Invite strangers and contacts who are not part of the SN.

6.10.2 Hosting of users on the home page

A very distinct feature of sOcialistOnline is that it hosts up to twenty recent users (followers) on the home page of a user (figure 18). While this may not be seen as a serious security measure, it provides additional information on users that log in onto the SN within a particular time frame, especially if the SN is customised for a small community like a university.

Figure 18: sOcialistOnline – Screenshots of recent followers (own compilation)

6.10.3 Private messaging

Private messaging (Appendix G-IV) is a solid feature that keeps users coming back to the SN. Although not as invasive as email, it is a simple functionality that enhances communication between a user and individual in his friend list across the SN. sOcialistOnline takes advantage of this functionality to keep its users happy and chatting securely with each other.

6.10.4 Other features of sOcialistOnline

Other features of sOcialistOnline include, but are not limited to, the following:

1. Email validation is done.
2. Lost passwords can be retrieved.
3. Friendship maintenance (add, accept, remove friends).
4. Send and receive messages.
5. Thoughts (users write what they are thinking on the wall for everybody to see).
6. Comments (every user can comment on anybody's thoughts).
7. Articles (users can write articles for everybody to read).
8. Blogs (users can send blogs to any group of his choice).
9. Chatting with other users.
10. Users can post photos onto their walls.

6.11 Summary

This chapter discussed the development and implementation of sOcialistOnline – the SN used for this research study. This SN is secured by technical and awareness techniques before being migrated to production. Similarly, the UAT and system testing were performed but limited to the postulated model and the conclusion is based on the evaluation of data obtained. Different types of technical controls, which form part of the body of a safe SN, are evaluated as well with special emphasis on the incorporated awareness techniques.

Although a safe SN is ultimately designed and migrated to life, the chapter was particularly interested in the awareness techniques used to secure the SN, because they are the main input data to the overall aim (section 3.2) of this study. The effectiveness of these controls and techniques proposed and implemented in this chapter shall be subjected to absolute measurement using the proactive approach, which is the major objective of this study. The

author, therefore, channels the remaining parts of this work to data-gathering, processes and procedures required to measure the effectiveness of these security techniques on the SN.

CHAPTER 7 DATA GATHERING AND AWARENESS MEASUREMENT

7.1. Introduction

The related works reviewed in Chapter 2 provides substantial theoretical and technical indications of the need for a proactive methodology to measure awareness efforts. This chapter 7 is core to this study because it employs an approach that is not based on incident statistics to evaluate the effectiveness of the awareness efforts implemented in sOcialistOnline in Chapter 6.

In this chapter, the author aims at two different but related goals. Firstly, he gathers both primary and secondary data relevant to this study and, secondly, he measures the effectiveness of awareness techniques on the SN using an approach that is not incident statistics driven. This chapter combines the second and third stage of this work following the development and implementation of sOcialistOnline to identify the possible impact of users' habits and normative beliefs (which are usually characterised by intentions and KAB) on security behaviours of SN users. The information obtained, analysed and measured in this chapter are the major points of discussion for this work, and the basis of this research findings.

The arrangement of this chapter is done in such a way that section 7.2 develops and employs a password cracker on the existing material, which includes the user passwords and photos obtained from the SN's password file. Section 7.3 administers the research questionnaire in the form of a quiz template, while section 7.4 is all about the survey and its two phases – KAB privacy and intention-gathering. Section 7.5 summarises the whole chapter.

7.2. Existing material – Stage 2

The first sub-phase of the data-gathering stage focused on the collection of existing data already gathered by sOcialistOnline. These are users' personal and confidential data, including photographs and password files. This process called for refining the research aim and developing a password cracker based on literature study and some other relevant studies highlighted in section 3.7. To ensure data collected from the study is treated as private and confidential, and to comply with UNISA's research ethics policy (http://www.unisa.edu.au/policies/codes/ethics/ethics.asp), the cracker displays only the security information about passwords without actually showing the password itself.

Recently there have been several sites (such as OnlineHashCrack 2013, Pendriveapps 2013, Stock & Barto 2013) offering to crack Facebook accounts, even at no cost. Some claim to crack SN users' passwords using the expertise they gained in the last few years, while others based their claims on their full awareness of the existing loopholes of Facebook and some other popular SNs. The truth is that Facebook does not use MD5 for password-hashing; instead, it uses a more complex system (OnlineHashCrack 2013:Internet). However, to prevent outsiders from cracking sOcialistOnline, this author rather implemented a system that is more complex than MD5.

7.2.1. The goal of the password cracker

People generally do not see legitimate reasons behind the creation of password cracker. However, the problem is actually not the existence of password crackers, but their frequent illegal use by fraudulent people for bad goals and objectives. When employed for good intentions, password crackers can offer a valuable service to system and data administrators by alerting them of system or users' weak passwords (Taber 2011:25)

Thus, the goal of password cracking is to provide a useful direct quantitative measure of the attitude and behaviour of SN users. Following the successful cracking of users' password files, the proposed solution in this study analyses the strength of individual passwords, using an automated statistical approach. The number of users using easily guessable passwords is a key indicator of effective awareness (section 2.5.2.2).

7.2.2. Selecting the most suitable password cracker

This section reviews some notable available password crackers in order to select the most suitable one for this research exercise. As mentioned in section 7.3, there are so many applications available to crack SN's password files, especially when the file is hashed with a less complex system such as MD5. These password crackers include, but are not limited to, Facebook Password Sniffer, John the Ripper, Password Decryptor, Google Password Decryptor, Password Security cracker, PasswordFox, Sniffer, OperalPassView, Access PassView, Web PassView, and AsterWin IE. Specific functions of some of the most current password crackers are analysed in table 11.

While trying to test the suitability of using the Facebook Password Decryptor as a cracker for this study, the author relaxed the hashing security on sOcialistOnline, and applied the Password Decryptor on the password file. The output was a good result as only the password security information and not the password combination itself showed. However, this may eventually be

counterproductive, because even if users' passwords are not displayed, the cracker must keep all the passwords before analysing the security information. Since Password Decryptors are mostly freeware, a desperate hacker may deploy it to gain unauthorised access to sOcialistOnline, thereby posing serious security threats and privacy risks. For this security reason in particular, it becomes necessary to develop a password cracker and analyser specifically for this study.

Table 11: Some notable password cracker (own compilation)

Password cracker (as at May 2013)	Description	Latest date of review
AsterWin IE produced by NirSoft (Pendriveapps 2013)	It uncovers passwords on Internet Explorer that are hiding or masking behind asterisks on the login pages. It is effective when exposing Outlook Express e-mail account passwords, and thereby revealing the hidden password by converting the password text boxes to normal text boxes.	November 11th, 2010
Cain & Abel (Stock & Barto 2013)	A well-documented tool that makes use of dictionary, brute-force and cryptanalysis attacks to crack encrypted passwords. It reveals password boxes and decodes scrambled passwords, by exposing cached passwords and evaluating routing protocols.	February 16th, 2012
Facebook Password Decryptor developed by SecurityXploded (Stock & Barto 2013)	It is highly recommended for a quick recovery of Facebook Account Login Passwords. It cracks for applications and web browsers on the system used to login to Facebook, and then attempts to recover or decrypt the password for each given login.	February 20th, 2013
Google Password Decryptor developed by SecurityXploded (Stock & Barto 2013)	This tool is handy in recovering lost Google Account Passwords. It is also useful to reveal, decrypt, or recover passwords for Twitter, Picasa, Gmail, GTalk, iGoogle, Desktop Search, and some other Google based applications.	March 17th, 2013

Password cracker (as at May 2013)	Description	Latest date of review
John the Riper made by Solar Designer	Although primarily built to detect weak Unix/Linux passwords, it also supports hashes for SNs and many other platforms.	September 20th, 2012
LOphtCrack	Equipped with several methods guessing password like brute force or dictionary, the tool attempts to crack Windows passwords from hashes obtained from networked servers, primary domain controllers, or Active Directory.	January 9th, 2011
Mail Password Recovery (Pendriveapps 2013)	This tool helps to retrieve email passwords for any POP3 account provided it is kept in an email program. By just changing the pop3 server to 127.0.0.1 for the e-mail account on which the password is to be retrieved, the tool displays and records the password to fetch the targeted email.	Not yet reviewed
MessenPass produced by NirSoft (Pendriveapps 2013)	It is used to reclaim the lost passwords from the current logged-on users of MySpace, Windows Messenger, MSN Messenger, Windows Live Messenger, Google Talk, Yahoo Messenger, AOL Instant Messenger, ICQ Lite, AIM and Miranda.	July 31st, 2011
Password Security cracker by NirSoft (Stock & Barto 2013)	It tests the passwords security stored in messengers, web browser and e-mail clients. Detailed information on every password stored is displayed, without disclosing the passwords itself.	March 29th, 2013
Password Unmask (Pendriveapps 2013)	This is better used to unmask hidden or lost passwords on any Windows 95, 98, ME, NT, 2000 or XP program, but not on most applications in Windows Vista. This tool may be stored and run from a USB Flash Drive or other a portable devices.	Not yet reviewed

Password cracker (as at May 2013)	Description	Latest date of review
PasswordFox produced by NirSoft (Stock & Barto 2013)	The tool discloses the names and passwords stored in Firefox. The password information such as fields and strength are displayed and may be exported to a file.	January 29th, 2013
Pphcrack	Although it runs on Linux and Mac, it is a table-based cracker specifically meant for SN's and Windows passwords.	March 7th, 2013
RainbowCrack	Unlike traditional brute force cracker, this tool makes use of a time-memory trade-off for the cracking-time computation, and stores the results in rainbow tables. It is faster than a brute force cracker once the pre-computation is completed.	August 26th, 2010
WebPassView created by NirSoft (Pendriveapps 2013).	Mostly used to recover forgotten usernames or lost passwords, which are stored within Google Chrome, Mozilla Firefox, Internet Explorer, and Opera Web Browsers. Recovered information can be saved to a text, html, csv, or xml file.	Not yet reviewed

7.2.3. Developing the cracker

A review of the existing crackers and analysers did not provide any suitable cracker to capture the logon details of users on sOcialistOnline, which includes passwords and user-Id. Many researchers have developed numerous crackers to crack and analyse user passwords of SNs. However, none of these solutions have ever worked with applications that do not use MD5 for password hashing (OnlineHashCrack 2013:Internet). Therefore, the author had to develop a new password cracker suitable for this research purpose.

This newly developed cracker, which is a utility software, can also crack and display security information of the passwords (and not the password itself) stored on Microsoft Outlook, Mozilla Firefox, and Internet Explorer and displays password security information such as password strength. This information shall be used to determine the strength of passwords used by the users of sOcialistOnline, without necessarily seeing the passwords themselves. Some of the features of the cracker are described as follows.

1. **System requirements/security:** This cracker is restricted to work only on Window 2000 version and up to Window 7, which are operating systems whose security settings are considered effective. Although hashed with MD5 system which is currently regarded as indecipherable, the newly developed cracker is stored and run offline from an external disk to wall it off from possible exploitations by a desperate hacker.

2. **Applications supported:** This cracker was incidentally tested and found suitable to crack the passwords of Internet Explorer 7.0 - 9.0, Internet Explorer 4.0 - 6.0, and Microsoft Outlook as well.

3. **Known limitations:** Only two limitations were noticed: (1) once protected by a master password, this cracker cannot crack Firefox passwords; and (2) Windows passwords can only be uncovered if the cracker is run with administrator's privileges.

4. **Columns description**: The cracker output has eight columns namely: user name, uppercase, lowercase, numeric, special, password length, repeating, and password strength. The columns are displayed in figure 19 and described as follows:

Figure 19: The screen-print of the password cracker (own compilation)

User Name	Uppercase	Lowercase	Numeric	Special	Password Length	Repeating	Password Strength
Johnson	0	0	5	0	5	0	Very Weak
admin	0	0	5	0	5	0	Very Weak
olayemi	0	6	0	0	6	0	Very Weak
jezz	0	6	0	0	6	0	Very Weak
ojoja	0	7	1	0	8	0	Medium
jamopow	1	7	1	0	9	0	Strong
owoblow	0	9	0	0	9	0	Weak
messi	0	0	10	0	10	0	Weak
rolex	1	7	1	0	9	0	Strong
adex	1	7	1	0	9	0	Strong
neyor	2	10	1	2	13	2	Very Strong

User name: The user name or UserID of the particular password item.

Uppercase: The total number of characters with uppercase (A - Z) in a password.

Lowercase: The total number of characters with lowercase (a - z) in a password.

Numeric: The total number of numerals (0 - 9) in a password.

Special: The total number of characters that are non-alphanumeric in a password.

Password Length: The total number of letters or characters in a password.

Repeating: The total number of characters repeated in the password. For instance, if the password is cnbnckc, the repeating value will be two since only c and n characters appear more than once.

Password strength: This may be calculated based on the total number of parameters including the character type, the presence and the total number of characters and repeating characters used in the passwords. Each value appearing in this column denotes the strength of the password, in line with the classifications in table 12.

Table 12: Password classification (own compilation)

Security classes	**Sub-classes**	**Class Interval**	**Character composition**
BAD	Very weak	1 - 5	Less than 8 characters length, only alphabets or numbers.
	Weak	6 - 15	Only alphabets or numbers but longer than 7 characters.
GOOD	Medium	16 – 29	Alphabets (lowercase or uppercase) plus numbers and longer than 7 characters.
	Strong	30 – 49	Uppercase, lowercase plus numbers and longer than 7 characters.
	Very strong	50 and above	Uppercase, lowercase, numbers, plus special characters (#, $) and longer than 7 characters.

It can also be inferred from table 12 that a password combination is:

1. bad and guessable if its character combination is weak or very weak; and
2. good if its character combination is medium, strong, or very strong.

Data related to the biographic details were eventually captured and stored for possible use in analysing survey reports. These include group, age, gender, tribe, country, qualifications,

profession, and technological advancement based on the user level of computer literacy and proficiency.

7.2.4. Performing the cracking

In line with this study timeline, sOcialistOnline was developed and system-tested in September 2011, but it was not migrated to production stage until November 2011 due to UAT and security challenges (addressed in section 6.7.1). The SN was planned to run for only 12 months (December 2011 – November 2012) but because of low patronage owing to low user' awareness, it was left at production stage until July 2013. Meanwhile, the password cracker has been developed and tested satisfactory for use since November 2012.

The sOcialistOnline password file that warehouses all the users' passwords was decrypted, downloaded and cracked into a flat data file. However, bearing in mind that not all people that sign onto the SN will remain active, the file was reviewed automatically to eliminate the non-active users. The cracker statistically analyses the compositions of the active passwords to determine their strengths and weaknesses as very weak, weak, medium, strong, and very strong.

7.3. The survey

It is expected that some SN users still use guessable passwords despite their high levels of awareness. This could be attributed to habit, normative beliefs, objectives, experience, and some other factors. In this study, awareness raising content is provided in the form of a quiz template (Appendix H) and each quiz comes with introduction text included on the same page. The quiz template is emailed only to users with very weak, weak, and medium passwords as defined in section 7.2.3 (table 12) asking them for responses.

7.3.1. The objective of the survey

The main objective of this survey/quiz is to identify the possible impacts of those control metrics that will be highlighted in section 7.4 in the findings of this research. This will be used as an additional tool to measure the effectiveness of technical controls and awareness in the SN. Therefore, keeping in mind this goal and objective, this author decides in the next section, whether to:

- Make use of any of the available crackers. In which case, the security on the password file has to be relapsed only to give way for the cracking exercise; or
- Develop a strong password cracker capable of cracking SN passwords that is hashed with a more complex system.

7.3.2. Developing the web quiz – questionnaire

An in-depth literature study could not produce any questionnaire suitable to capture awareness contents of SN users that include normative beliefs and habit. Surveys such as Guenther (2001), Manly (2013), and SANS (2012) have been done on awareness, but these questionnaires did not offer the information and data needed to explore relationships between user behaviour, cultural dimensions, and awareness. Surveys from awareness metrics were found useful to some extent, in particular that of Mitchamz (2013). However, none of these studies cover the scope of this study and only individual questions could be recycled.

This author eventually consulted the recent literature and commercial information regarding human behaviour towards the use of SNs to compile a questionnaire, which is transposed to a web quiz for this study. Data related to the following measurement dimension of awareness (section 5.6.1) and some other facets were captured and analysed:

1. **Knowledge:** Password-handling, virus prevention and controls based on the users' basic understanding of security perspectives as related to awareness.
2. **Attitude:** Privacy concerns on security, SN settings, and self-hiding of profile data. These are important security issues, which a user may or may not believe in. It is purely based on the user's belief about IS safety and privacy on the SN, and the priority a user gives to security type (economic, reputation or physical).
3. **Behaviour:** How a user protects his sign-on, safeguards information, controls and sets his privacy, reads and understands the SN's policy before signing on. It may also encompass users' reaction to general email and internet issues with respect to awareness. These are user styles of living or work, which is insecure upon his adequate knowledge of awareness.
4. **Normative beliefs, needs, objectives and experience of the SN's user:** It was decided on the basis of literature study that upon the priority given to awareness (KAB) as the most important facet of information security noted, collecting data on users' normative beliefs and objectives, security exposures and attacks would aid the survey to achieve its goal and add value to this study.

7.3.3. The participants

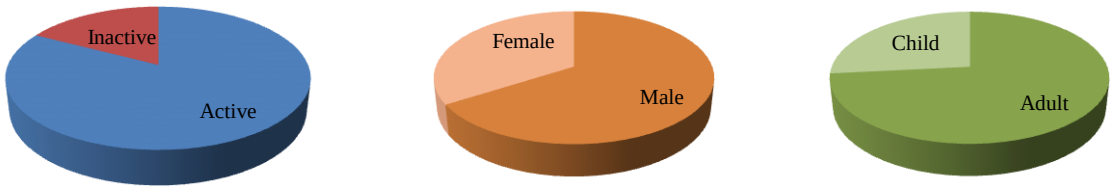
Out of the total population of 2,436 users on sOcialistOnline as at July 8, 2013, only 2,015 users were active, representing almost ratio 5:1 against (421) inactive participants. That is:

$\{2{,}436 - 2{,}015\} = 421$; and

$(2{,}015 : 421) =$ **5 : 1.**

In order to obtain a more reliable result and to abide by government regulations regarding children completing questionnaires, the survey is restricted to only the teenagers and adult participants; in which case, 112 users below the age of 13 years were further eliminated from the active sample size. The study therefore has a final population size of 1,903 active participants (adults and teenagers), 66% male and 34% female. The participants are mostly students from Nigeria and a few other African countries, with an average age of 22 years between 13 years and 53 years. These population distributions of the SN users are as represented by the following pie charts in figure 20.

Figure 20: SN users' population distribution ratios (own compilation)



a.) Active vs. Inactive. b.) Male vs. Female c.) Adult vs. Child.

7.3.4. Conducting the survey

Conducting the survey in this context is, therefore, referring to the administration of the quiz template (Appendix D) to the participants with bad password combinations, requesting their responses. As will be discussed in Chapter 8, the population size of this class of bad passwords is 364. However, since this exercise was voluntary and no incentive is provided to the participants, 52 participants failed to respond to the quiz thereby bringing the class size to 312. This quiz consists of only 20 questions, five each from the *knowledge*, *attitude*, *behaviour*, and *user needs and objectives* categories.

Given that the survey can be conducted with the administration of either the questionnaire or interview (Olivier 2004:3), the author chooses to apply the four principles of contextual interviewing as postulated by Holtzblatt and Beyer (2005) to guide the quiz administration process. These principles, which include context, interpretation, partnership, and focus are described as follows:

- **Context**: Data were collected on how the individual manages his access to the SN by closely observing how long their system is left idle when their logon is still active on sOcialistOnline, and asking them questions with regard to their behaviour.

- **Partnership**: The author collaborated with users to appreciate their behaviour and thinking, by raising some questions that may entice the SN users to complete the quiz without a hitch.
- **Interpretation**: Multiple-choice questions were raised all through to avoid misinterpretation of respondents' words and logon behaviour.
- **Focus**: The project keeps to its focus by restricting the quiz to only active users with weak, very weak, and medium passwords.

All the participants were exposed to the same set of questions. By a covering memo popping out at the first page of the quiz template (Appendix H-ii), they were all informed that the exercise is optional and that its objective was to ascertain that their insecure behaviour on the SN is not attributed to inadequate awareness efforts. The information gathered at this phase was analysed further to form an opinion.

7.4. The quiz template/questionnaire

The first phase of this study was discussed in section 7.2, where a proactive approach was used to crack and analyse user passwords in order to measure the impacts of awareness techniques highlighted in section 6.6. The survey is the second phase and comes as a questionnaire to determine those factors that are capable of infringing the validity of findings of this study. This section, therefore, aims at investigating the possible impacts of KAB and user intention in the effectiveness of awareness on SNs. This comes in two phases – survey of privacy KAB, and intention-gathering.

7.4.1. Survey of privacy KAB

The survey was designed to measure KAB, which are the three dimensions of awareness. This section surveys the user's privacy priority, password security management, confidence in existing SN settings, compliance to SN policy, user habits and behaviour (Appendix D). Questions 1 to 15, representing 75% of the questionnaire, address KAB, while only 25% focus on intention and some other factors. The survey tests the knowledge, attitude and behaviour of SN users towards security-related questions and situations. Although it is beyond the scope of this study, the results of the survey may throw more light onto those aspects of awareness that call for improvement, and assist further in computing a risk level of an SN. The target of this type of survey can ordinarily be used to determine the area of awareness that needs improvement, and to calculate the risk score for each security dimension or the probability of an SN user compromising the system (Bond 2012:1). The risk score in this study is used to

determine the validity of the research findings by evaluating whether or not implemented awareness efforts can be influenced by KAB, intention and other related factors.

Some of the optional answers to each of these multiple questions denote strong awareness and good practices, while others signify insecure attitudes and behaviour of higher-risk activities. On this basis therefore, risk/significant value is assigned to each question's response, ranking from one to four with "one" being the lowest and "four" being the highest risk/significant level. When collated and properly analysed, the result of the significant level is used to determine the influence of each of the KAB elements on awareness following the following equations derived by the author.

1. Multiply respond risk value (1-4) of each of the 20 questions in appendix D by the number of participants that answer it, which is the number of times a particular question is chosen (since no participant is allowed to answer a question twice). That is,
   {Response risk value} X {number of times chosen} => Response total .....equation 1.

2. Sum up the response total (RT) for each of the questions to obtain the cumulative response total (CRT) value.

$$\sum_{k=1}^{5} (\mathrm{RT})\,\mathrm{k} \quad = \quad \mathrm{CRT} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{equation 2}$$

   Where k is an integer count to the tune of five questions for each of the security dimensions (knowledge, attitude, behaviour and intention/others).

3. Divide the survey cumulative response total (CRT) derived in equation 2 by the number of survey-takers (NST) to arrive at the risk score (RS) for each of the security dimensions.

$$\frac{\mathrm{CRT}}{\mathrm{NST}} \quad = \mathrm{RS} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{equation 3}$$

4. Sum the risk score per subject area to obtain the cumulative risk score (CRS) for each of the KAB dimension and intention.

$$\sum_{j=1}^{4} (\mathrm{RS})\,\mathrm{j} \quad = \quad \mathrm{CRS} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{equation 4}$$

5. Using the calculated cumulative risk score (CRS), cross-check the risk levels in table 13 to determine the SN's general risk rating.

Table 13: The potential risk levels (own compilation)

Risk levels	Range	Description
Low	1 – 6	SN's users are fully aware of security policies and procedures, the potential risks and possible consequences of a threat. They have all the trainings and exposures to mitigate an attack.
Elevated	6 – 9	Users have a good understanding of awareness with adequate exposure but they may choose not to comply with good security policies, principles and controls.
Moderate	9 – 13	Users are aware of security threats and potential attacks but they have knowledge gap in identifying or reporting security events and therefore require training and exposure.
Significant	13 – 17	Users understand security policy and standard but they do not believe they are truly accountable for their security performance. They assume security lies in technology and the management of the SN.
High	17 – 20	Users are not interested in controls and security for reasons only known to them. They exhibit risky behaviour that can be easily exploited, thereby making the SN more vulnerable to various attacks.

Since each security dimension contains five questions with minimum score of one and maximum score of four, then

Minimum risk score = (5 x 1) = 5; and

Maximum risk score = (5 x 4) = 20.

7.4.2. Gathering of intention

The intention of any user to share information just like in a typical access control decision, depends greatly on both the information to be shared and the individuals to share them (Madejski, Johnson & Bellovin 2011:3). This author comes up with a table of profile groups and information category (table 14) to collect the KAB and the sharing intentions of participants per information category per profile group to determine their possible influence on the result obtained when measuring awareness efforts with an approach that is not incident statistics driven.

Table 14: The profile groups and information category (own compilation)

Information category	A sOcialistOnline friend	Not a sOcialistOnline friend	A sOcialistOnline member but not a friend	A friend of a friend on sOcialistOnline
Academic (School, lecturer, etc.)	Show Apathetic Hide	Show Apathetic Hide	Show Apathetic Hide	Show Apathetic Hide
Work (Employer, interview, etc.)	Show Apathetic Hide	Show Apathetic Hide	Show Apathetic Hide	Show Apathetic Hide
Personal (photos, age, gender, etc.)	Show Apathetic Hide	Show Apathetic Hide	Show Apathetic Hide	Show Apathetic Hide
Family (Mum, uncle, siblings, etc.)	Show Apathetic Hide	Show Apathetic Hide	Show Apathetic Hide	Show Apathetic Hide

With each column and row representing each profile group and information category respectively, this table was sent via email to the same set of participants (the questionnaire-takers) with bad password requesting for their sharing intention whether Show, Hide or Apathetic. Ordinarily, most privacy interfaces present only two mutually exclusive options to display or conceal information (Madejski et al. 2011:3). However, apathetic is included in this instance, since there exist situations where respondents are indifferent either way. Thus, it is considered as a good alternative option when sharing intention is being recorded. A description of profile groups and information categories in this context is as discussed below.

7.4.2.1. Profile groups

Similarly to Facebook, the sOcialistOnline configuration option is displayed on the basis of default profile group (friends, strangers, SN members, or friends of friends), which are manually configured. However, this study is restricted only to the default group settings.

A friend is someone who is already confirmed as a friend by another user while a stranger is someone that is not yet a friend of any friend. An SN member is someone on the SN that shares SN membership with another user on the same SN while a friend of a friend is a user who, on the same SN, is a friend to one of the user's friends (Madejski, et al 2011:4). In reality, it is very possible for these groups to overlap but this study consider profiles that fit only into one of the profile groups.

7.4.2.2. Information categories

SN generally allow configuration of privacy settings for both the basic information and each data type. The basic information fields are often static, and include gender, name, date of birth, and nationality, with each of them having a separate setting. Conversely, data types are more dynamic in nature, and include photos, addresses, events, links, and status updates. In which case, to ensure adequate protection, users can select default settings for each type, and/or set privacy controls for every data object that is being submitted.

Information is usually categorised in classes (personal, private, public, etc.), which reflects how sensitive they are. This study selects information categories on the basis of the subject areas that can possibly influence users intent to show or hide from a profile group. Each category has a list of keywords, manually generated using specific words that are common to them. The categories are not exhaustive, as the scope of this work does not cover the upper bound of SN's privacy violation. Hence, the information category is limited to the following list but with more keywords per category:

1. **Academic:** School, course, homework, lecturer.
2. **Work**: Employer, interview, promotion.
3. **Personal**: Nickname, address, age, gender, marital status.
4. **Family**: Father, sister, mum.

7.5. Summary

Following the needs for a preventive technique to measure awareness on SN as discovered from the literature reviews in the earlier chapters of this study, this chapter considered the concept of data-gathering and provided an overview of a proactive approach of measurement. This is what the second and third stages of the entire research is all about, and it was achieved in just two steps.

First, the available information on the password and object files obtained from the SN users was cracked to determine the strengths of individual passwords. Secondly, a quiz template of awareness raising contents is provided and administered only to users with guessable password combination. This is to establish the possible influence of KAB and intentions of the SN users on awareness efforts and, in particular, on the findings of this study.

Data and other relevant information gathered from this chapter will be good sources for the findings and the results that shall be adequately reviewed, discussed and analysed in the next chapter, pending conclusion and final recommendations in Chapter 9.

CHAPTER 8 FINDINGS AND DISCUSSION

8.1. Introduction

The goal of this study was to develop and implement a technical control – a technique that is not based on incident statistics– to measure the effectiveness of awareness techniques in SNs. It also aimed at measuring the impact of security dimensions (KAB) on awareness. With regard to objective 2, the study desired to ascertain the influence of information categories (personal, family, etc.) on awareness efforts (sections 7.4.2 and 7.4.2.2); and to determine the privacy intentions of SN users and their impacts towards improving awareness. Secondary objectives also intend to develop a set of preventive evaluation criteria to measure the impacts of awareness on SNs, and to subsequently target further users' awareness training, where and when necessary.

This chapter, therefore, presents the graphical, tabular and narrative information of these research findings, and recaps the objectives to discuss the results obtained.

8.2. A proactive approach

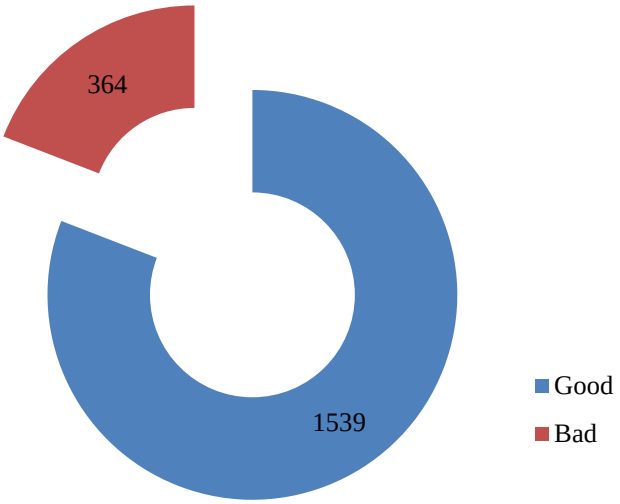
This section discusses the major finding and objective of this study. The result from the password cracking exercise in section 7.2.4 is summarised in table 15, where the numbers of good and bad passwords are almost at ratio 5:1 with bad password taking less than 20% of the total population size.

Table 15: Output from the password cracker (own compilation)

Password classes	Good	Bad	Population size
Very weak		135	135
Weak		229	229
Medium	384		384
Strong	397		397
Very strong	858		758
TOTAL	1,539	364	1,903

As indicated in table 15 and figure 21, only 364 passwords out of the population size of 1,903 are considered bad passwords, implying that the percentage of users with weak and very weak passwords is very low when compared with other past related findings as established by various past literature reviewed.

Figure 21: Good vs. bad password combinations (own compilation)



This is an improvement on the work of Samuel and Samson (2012), where the relationship between good and bad passwords was almost at par. In their research concluded in March 2012, they suspected that inadequate awareness was the main factor behind the users' insecure behaviour on the SNs. They concluded that if they had improved on their awareness efforts, the SN users would have understood the security implications of poor password combinations, and, therefore would have complied accordingly with security principles and practices. For this reason, the success recorded so far in this study may be traced directly to various adequate and effective awareness techniques implemented on sOcialistOnline, some of which are described in section 6.6 including Explicit Privacy Policy, Privacy Awareness and Customisation, Data Minimisation, Privacy Lens, Password Monitoring and Standardisation.

The major achievement here, which remains the main focus of this research, is that the effectiveness of awareness efforts implemented on the SN was successfully measured using a technique that is not incident statistics driven. The implication is that guessable password combinations could be discovered before the occurrence of an event or success of an attack.

8.3. Security dimension (KAB)

Table 16 depicts the results from the survey conducted on the SN users with guessable passwords based on the questionnaire/quiz provided (Appendix D). As indicated in section 8.2,

table 15 and figure 21, the total population size for users with bad passwords is 364. However, for reasons stated in section 7.3.4, the analysis of the quiz result is limited to only 312 respondents. The column description for the result is as presented in the table below.

Table 16: Results from the questionnaire (own compilation)

	Question's nos.	No of time chosen	Cumulative response total (CRT)	Risk score (CRS/312)	Risk level
Knowledge					
	1	312	404	1.29	
	2	295	313	1.06	
	3	302	442	1.46	
	4	245	295	1.20	
	5	278	287	1.03	
	CRS (K)			**5.58**	**Low**
Attitude					
	6	285	1,049	3.68	
	7	312	897	2.88	
	8	291	952	3.27	
	9	278	992	3.57	
	10	287	778	2.71	
	CRS (A)			**14.96**	**Significant**
Behaviour					
	11	248	384	1.55	
	12	312	1,120	3.59	
	13	289	853	2.95	
	14	307	850	2.77	
	15	311	1,145	3.68	
	CRS (B)			**13.95**	**Significant**
Intention/Others					
	16	299	903	3.02	
	17	297	615	2.07	
	18	304	887	2.92	
	19	287	720	2.51	
	20	300	786	2.62	
	CRS (I)			**12.54**	**Moderate**

1. First column: The description of what a particular question is all about.

2. Second column: The serial number of the quiz questions specifically meant to identify the question.

3. Third column: The total number of times each of the questions was answered by the respondents. It is surprising to note that only questions 1 and12 were fully attended to by

all **312** participants; the rest are far below 312 with question 4 being the least attended to. Although this does not have an impact on the result obtained, it confirms that the total number of survey-takers in this context is 312, since no participant can answer a question more than once.

4. Fourth column: This is the column that contains the summation of response total for each of the questions. The computation of both response total (RT) and cumulative response total (CRT) is done with equation 1 and 2 respectively, and is discussed in section 7.4.1.

5. Fifth column: This is the column for total risk score per survey question. The RS is computed using equation 3 in section 7.4.1, and the summation of the total risk score (RS) per survey question gives the total calculated cumulated risk score (CRS) for each security dimension. This is denoted as CRS(K), CRS(A), CRS(B) and CRS(I) for knowledge, attitude, behaviour and intention respectively, and is compared with Risk Levels on table 13 to measure the general risk rating of the SN. Please note that the number of survey-takers (NST) in this case denotes the total number of participants that took parts in the security survey, which is 312.

Relating the computed CRS in table 16 to the ranges of potential risk levels on sOcialistOnline, it is interesting to note that knowledge is the only security dimension that does not pose a serious security issue. Knowledge with CRS(K) = 5.58 presents low risks to the SN, implying that users generally have a good understanding of awareness with adequate exposure, even though they have chosen not to comply with good security policies, principles and controls. Conversely, if CRS(K) > 12 implying a moderate, high or significant risk, then it will be an indication of a wide security knowledge gap on the part of the SN users, which could have had some negative influence on the findings of this study. Consequently for a single reason that awareness is adequate, the measurement of awareness efforts in section 7.4 using a proactive approach (which is the main focus of this study) is **not** being influenced by users' knowledge.

In a similar vein, it can be deduced from the same table 16, that SN users' attitude, behaviour, and intention/others each have a CRS > 12 which is moderate, high and significant enough to pose a serious security threat on the SN. Given that SN users are knowledgeable on awareness as evidenced by CRS(K) < 12, some in this category still do not believe that security depends on the users but on technology and the management of the SNs. Other users have faith in security and controls but they are just not interested for reasons not yet understood. They exhibit risky behaviour that can be easily exploited thereby making the SN more vulnerable to various attacks.

This agrees with Adams and Sasse's (1999) position that irrespective of the adequacy of user's knowledge, there are other major factors influencing users' security behaviour, including multiple passwords, perceived compatibility (between practices and password procedures), and users' perceptions to security. SN users "having a large number of passwords reduces their memorability and increases insecure work practices, such as writing passwords down". Users perceive their behaviour to be caused by a mechanism designed to increase security. At the same time, users devise their own methods for creating memorable multiple passwords through related passwords (Adams & Sasse 1999:43-44)

Inadequate awareness (knowledge) is not an issue in this study but rather habit, beliefs, and style of living. Consequently, users with an unfriendly attitude, unsafe behaviour and malicious intention will disregard their security knowledge and expose the SNs to various threats and vulnerabilities. Therefore whether or not the implemented awareness effort is strong and adequate, users' attitude, behaviour and intention may still render them useless. This explains why upon growing coverage of the importance of cyber-security in the media, a large proportion of Internet users still engage in insecure behaviour online (Khan et al. 2011:8) It also implies that knowledge can only measure the adequacy (and not the efficiency) of the awareness efforts. Hence, these same factors may have influenced the outcome of measurement of awareness efforts carried out in section 8.2 using an approach that is not incident statistics driven.

8.4. Information category

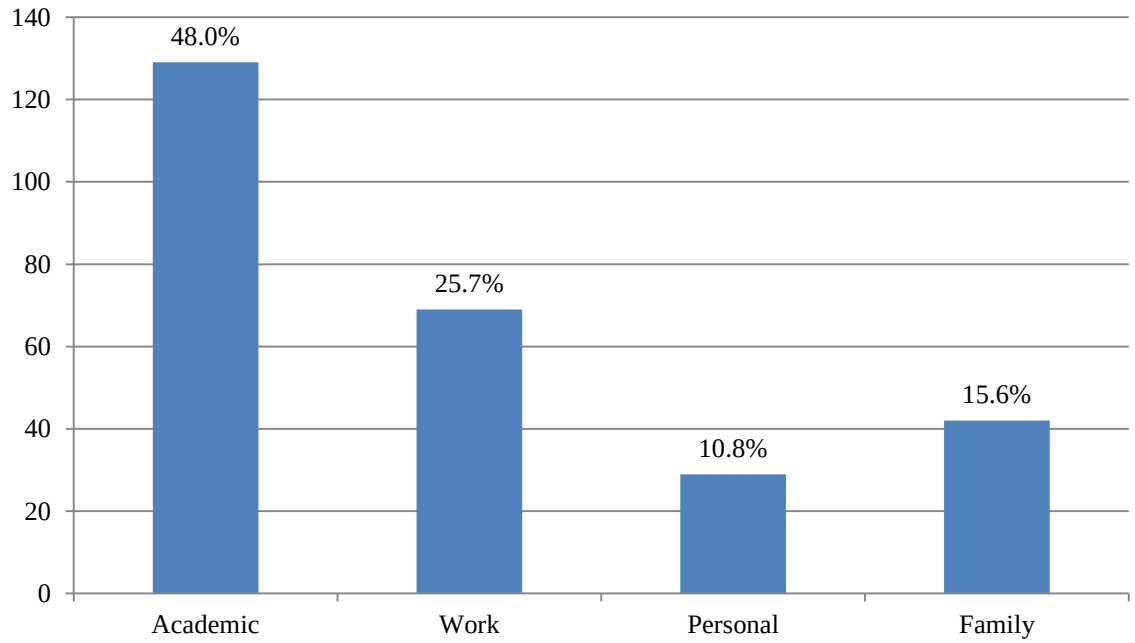
All 364 SN users with bad passwords (as defined in table 15) were invited but only 268 responded to the study requests (table 17). However, it is noteworthy that all the 268 respondents attended to all the questions on a table of profile groups and information category, making the data analysis easier for this work. In table 13, the participants were asked to choose among the four information categories their reasons for using an SN, and to identify their sharing intentions among the profile groups. The results obtained from this exercise are as depicted in table 17.

Table 17: Sharing intentions amongst profile groups (own compilation)

Information category	Sharing intension	Friend	Stranger	SN member	Friend of a friend	Sub-Total	TOTAL
Academic (School, lecturer, etc.)	Show	35	13	16	22	**86**	**129**
	Apathetic	2	5	3	1	**11**	
	Hide	5	11	6	10	**32**	
Work/Business (Employer, interview, etc)	Show	18	7	10	11	**49**	**69**
	Apathetic	2	1	2	2	**4**	
	Hide	3	4	3	4	**16**	
Personal (Photos, age, gender, etc.)	Show	6	3	3	3	**15**	**29**
	Apathetic	2	1	2	1	**6**	
	Hide	2	2	1	3	**8**	
Family (Mum, uncle, siblings, etc)	Show	8	6	5	5	**24**	**42**
	Apathetic	1	3	1	2	**7**	
	Hide	4	3	2	2	**11**	
							268

Figure 22 represents information categories for which participants intend to use the SN. Academic is by far the largest target for most interactions (with sum total sharing intention of 129) and very consistent across the profile groups, representing 48% of the population size (table 17). This tally with the questionnaire results obtained on question 16 (Appendix D) as represented in table 16 where academic was still the preferred option with CRT of 903. Even though only 299 participants among the questionnaire-takers (table 16) responded to question 16 in the quiz template (Appendices D), the CRT of 903 and RS of 3.02 for academics – which are the attributes that signify a degree of importance – remain the highest among its group members (intention/others).

Figure 22: Information categories by total population (own compilation)



Academic, representing a larger portion of interaction for information-searching may not be surprising because it can easily be attributed to the fact that:

1. 86% of the respondents are scholars comprising of students, lecturers and researchers; or
2. Regardless of how significant a risk score is, risk impact on academic data is always mild and may not be as severe as in other categories such as business, personal, or family data.

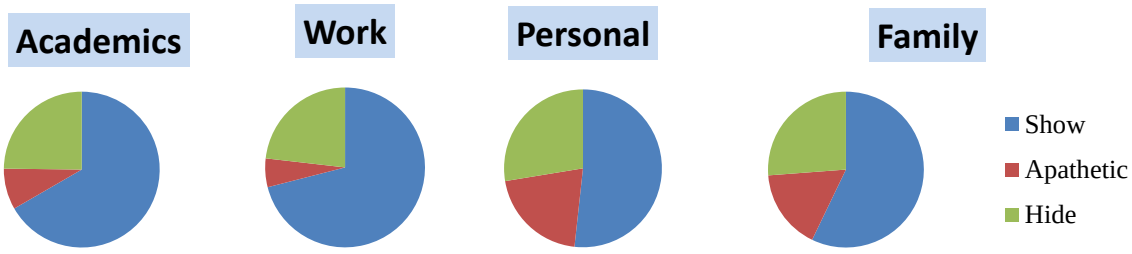
Consequently, these two factors may as well be parts of the major reasons why this group of people choose not to take security serious by neglecting the awareness and stick to insecure behaviour and poor password management. Hence, the information category or reasons for which a user intends to use an SN have a strong impact in determining his security behaviour and may make awareness efforts useless and ineffective.

8.5. Privacy intentions

Previous works (Day 2013; NCSA 2006; Rand 2007; Samuel & Samson 2012; Strater & Richter 2007) have actually shown that a greater number of adults tend to disclose their personal information such as email, work address, birthday, and even their social security numbers (SSN). While users on LinkedIn generally expose their private and confidential data on their profile (Rand 2007:9; Samuel & Samson 2012: 5), the majority of Facebook users are cautious of the information type they disclose (Day 2013:1). Users are getting more aware of personal privacy issues and are, therefore, tending to post mainly positive information on their identities, or restricting their private data from a diverse audience (Day 2013:2).

This study agrees in part with all these past works as could be noticed in table 17 where Show (with subtotal 86) is considered as the clearest intention of users willing to share information and resources. As also presented in figure 23, each chart represents the distribution of sharing intention amongst information category, and Show is overwhelmingly the largest target for all categories consistently representing the highest segments.

Figure 23: Sharing intentions amongst information categories (own compilation)



However, it is surprising that upon awareness efforts, which are adjudged effective as evidenced by the adequacy of security knowledge (presented in section 8.3), the majority of SN users still tend to disclose their personal and family information to strangers and ordinary SN's friends. This implies that only very few users are concerned about privacy, data access control, storage or distribution of their private information; and it may not necessarily be due to ignorance or inadequate awareness amongst the targeted population but deliberate or intentional (Dionysiou 2012:4). Hence, the indiscriminate sharing intention of this group to make their individual information available to almost every user is also one of the major factors that make them carefree about their choice of password combination. The privacy intention (Show, Apathetic, Hide) of SN users to share information is, therefore, a determinant factor for their insecure behaviour regardless of awareness efforts.

8.6. Evaluation criteria

The security and privacy challenges on the SNs lie on the SN providers, the third parties and largely, the users (Dionysiou 2012:2). Therefore, the investigation exercise of any researcher interested in the security links on the SNs have to be focused on all three parties as their actions have a strong influence on the overall security of the network. This is implied from the literature reviewed in Chapter 2 where more emphasis was laid on the importance of security and its measurements. Measuring security is paramount to ensure that controls are effective and working as intended.

While measurement evaluation criteria have been derived for SN providers, and the ones for third parties are still at the infant stage, none is yet available for users' awareness. According to some notable researchers, the criteria to evaluate the security of any SN include the capability to report spam, support privacy settings, report abuse, block user, and provide safety tips (Dionysiou 2012:2). The evaluation criteria for the third party will be subjected to future study as its discussion is out of the scope of this study. However, while knowledge is considered as the only factor that determines the adequacy of awareness efforts, findings obtained in section 8.3 and section 8.4 present users' attitude, behaviour, intention and information category as the evaluation criteria that determine the effectiveness of awareness on the SNs.

Section 8.3 establishes that knowledge does not affect the outcome of the research findings because users' knowledge is adequate due to effective awareness techniques implemented. This suggests that the research findings would have been negatively affected if the users' knowledge were inadequate, as a result of inadequate awareness efforts. The result of the findings was influenced directly by attitudes, behaviour and intentions of the SN users (sections 8.3 and 8.4), and insinuates that regardless of the strength of awareness efforts, these attributes may still render them useless.

8.7. Awareness training

The extensive review of the past related works in Chapter 2 emphasised the importance of awareness in securing SNs. Several security standards (ISO/IEC 27001, TCSEC, ITSEC, etc.) have also been advocating the integration of awareness and training programmes into organisational practices because training remains the most effective technique for raising awareness (ENISA 2007:8-13; Samuel & Samson 2012:4). Awareness training is indeed a persistent programme that calls for advanced knowledge to offer security basics and literacy to all SN users (section 4.3.1).

The theoretical foundation provided in Chapter 4 to address security threats and drivers of SNs further makes the need for awareness training to be more eminent since the classification of threats as internal or external may help to suggest further awareness training. However, the findings obtained from this research do not give a clue towards the need for awareness training, because the selected SN users already have an adequate knowledge of awareness. This agrees with Stanton et al. (2005:128) that there is no relationship between password-sharing behaviour and awareness or training.

The results obtained so far in sections 7.3 to 7.5 have proven that the factors that influence the effectiveness of awareness efforts on the SNs include knowledge, attitude, behaviour, information category, and user intention. Amongst all these factors, training can influence only user knowledge towards awareness and no more (Yngström & Jörck 2010:4), because other factors are habitual, and may remain perpetual regardless of training efforts. Consequently, since user knowledge is adjudged adequate implying that awareness efforts are adequate and sufficient, then, further user awareness training is not necessary.

8.8. Summary

The entire study is focused on the development and implementation of an approach that is independent of incident statistics to proactively measure the effectiveness of awareness efforts. This primary objective gave rise to five important secondary research objectives, all of which are addressed in this chapter. The results of the findings were discussed here to clarify and authenticate how these research objectives were met. This chapter validated this proactive approach of measurement by considering the research findings and results as related to the past relevant literatures review.

The next chapter is the last chapter for this study, and it is aimed at reflecting on the outcomes of this chapter to arrive at the overall conclusion. This chapter has provided an extensive background to the next one in order to proffer answers to all the research questions and to carry out the methodological, scientific, and substantive reflection on the research findings and objectives.

CHAPTER 9 REFLECTION AND CONCLUSION

9.1. Introduction

This final chapter aims at giving a summary of the study, reflect on the entire study and conclude with recommendations for future works. The chapter is organised as follows: Section 9.2 summarises the research findings by recapping the research sub-questions and responding to all. Section 9.3 specifically answers the primary questions while theoretical contributions of this study are highlighted in section 9.4. Bearing in mind what has been done and achieved in this study, section 9.5 reflects on what could have been done and the reasons this work was done as described in this thesis. This chapter justifies the scope of this work and discusses related aspects that were not covered in this study. Practical contributions of this study are detailed in section 9.6 before recommendation for future work is considered in section 9.7. Section 9.8 concludes this study.

9.2. Summary of the findings

In order to summarise this study, the research questions are recapped in section 9.2.1, and the respective findings and answers are provided in section 9.2.2. Table 18 is presented in section 9.2.3 to give an overview of the questions and answers at a glance.

9.2.1. Recapping research questions

The primary research question for this study as introduced in section 1.4 was:

> How can technical controls be used to measure the effectiveness of awareness efforts in SNs?

Subsequently, the following secondary questions were raised to unravel the issues and provide answers to the primary question:

1. What metrics can be applied to measure online user behaviour in SNs?
2. What controls are available to measure awareness?
3. Why should technical controls be explored as an option to measure awareness in SNs?
4. Can password cracking be used as technical control to measure awareness in SNs?
5. Will a quiz template be an appropriate tool for data collection on the SN?
6. Can a technical control that is not based on incident statistics be adequate to measure the effectiveness of awareness in SN?

9.2.2. Response to research sub-questions

This section will now consider the main findings as related to each of these research questions so as to offer appropriate answers to the questions.

9.2.2.1.

What metrics can be applied to measure online user behaviour in SNs?

The user, the most important security component, is seen as the weakest link in the Information System control chain (Bangkok 2010:Internet; Boss 2007:27; Van Niekerk & von Solms 2004:2), hence its behaviour demands adequate measurements. As elaborated in section 5.7.3 and 5.8, several metrics have been developed to measure awareness but none is specific to user behaviour. When applied to measuring user behaviour, the results have always been ineffective because there are so many influencing metrics (such as knowledge, attitude and behaviour) that are yet to be considered adequately. Some of these metrics to measure user behaviour were eventually discovered in this study.

The literature review in Chapter 3 delineated metrics as targets or criteria (but not methods of measurement) on which awareness efforts may be evaluated. Results obtained in section 8.3 identified determinant factors for users' insecure behaviour on SNs as knowledge, attitude, behaviour/belief, information category, and privacy intentions. Knowledge is the only factor that would have influenced the research findings if not for the adequacy of awareness (section 8.3); others are not affected in any way by implemented awareness efforts (section 8.3 – 8.5). Hence, knowledge cannot be a good criterion of awareness measurement since a user may still choose to exhibit an insecure behaviour regardless of his in-depth knowledge of awareness. By implication, therefore, the control metrics that determine the effectiveness of awareness efforts in SN will include attitude, belief, information category, and privacy intentions of users.

9.2.2.2.

What controls are available to measure awareness?

Several measurement controls are now in place and they are categorised by some researchers (ABC 2013; ENISA 2007) into internal protection, attack resistance, process improvement, efficiency and effectiveness. However, section 2.7 of this study agrees with Davis (2008) in isolating the controls into conventional, unconventional, security metrics and now, a non-incident statistics approach.

Conventional methods are more effective when used to measure intangible dimensions such as knowledge, attitude and behaviour. Typical examples are tabulated in section 5.7.1 and include surveys, interviews, focus groups, assessment tests, and behaviour measures.

Unconventional methods are often used to measure tangible dimensions such as to obtain users' passwords, examine network traffic, and detect phishing attempts. Instances are given in section 5.7.2 to include social engineering, software implementation, worm, and gaming software.

Security metrics refer to the use of evaluation criteria to measure awareness efforts. In this case, the author is not restricted to a single measure and may, therefore, apply multiple measures on the basis of overall pictures. Examples are listed in section 5.7.3 and include audit findings and ROI.

The non-incident statistics method is a new approach presented by this study. All the aforementioned controls are incident-driven and are applicable only when an event has happened or an attack succeeded. Password cracking is a typical example and have been confirmed effective when measuring awareness efforts in this study.

9.2.2.3.

Why should technical controls be explored as an option to measure awareness in SNs?

Literature reviewed in section 3.7.2 established that there are several conventional and unconventional methods to measure awareness efforts but that most of them are reactive and post-mortem. Some researchers (ABC 2013, Samuel & Samson 2012, etc.) therefore adjudged the methods as incident statistics approaches because the measurement of their effectiveness is often based on the occurrence of an event or success of an attack. These techniques are not acceptable especially in the airline sector where the risk-tolerance level is very low. Hence there is a strong need for a technical control to be implemented independent of incident statistics and be proactive against current security challenges on the SNs.

Several researchers (Asim et al 2010, Hinson 2012, and PriceWaterHouseCoopers 2010) have implemented technical controls on SNs but only as part of security measures to tighten access controls to both the information and the SN. This research eventually illustrates that technical controls are not only meant to secure SNs, but can be employed equally to measure the effectiveness of awareness efforts in SNs.

9.2.2.4.

Can password cracking be used as technical control to measure awareness in SNs?

A measurement approach is termed to be non-incident if it is proactive in nature and does not need to wait for an occurrence of an event or a success of an attack before being used. Obviously, password cracking falls into this category and it is indeed independent of incident statistics. It may therefore be classified as another form of vulnerability assessment tool that makes use of password attributes to determine the vulnerability of SN's users to the known attacks (Bace & Mell 2001:23). When implemented online real-time on an SN, it regularly cracks the password file and at logon, alerts the user of the insecurity in his passwords combinations. Depending on the implementation mode, it can be automated to send reminders to users with guessable passwords at a predetermined time interval, offering them an adequate awareness on the potential risks their information is exposed to.

All other methods discussed so far are post-mortem in nature. Rather than being preventive, they are reactive and can only be classified as detective or corrective controls. As an instance, social engineering, software implementation, worms, and gaming software are all good at collecting data on events that have happened for possible analysis. The same applies to surveys, interviews and behavioural measures. Nevertheless, when combined with a proactive approach, these reactive statistic methods may be used to authenticate the validity of the research findings just as we have in this research study.

9.2.2.5.

Will a quiz template be an appropriate tool for data collection on the SN?

Related research findings from some notable researchers such as Ganger and Jackson (2003), Segall, Doolen, and Porter (2005), Treadwell (2006), and Bonneau and Preibusch (2013) have ranked data collection methods using the test scores, efficiency, and participant satisfaction (Cheung & Hew 2009:160). According to their conclusions, there is not much difference in the test scores between the quiz and other methodologies such as pencil assessment. Similarly, the argument whether quizzes is more efficient going by the time it takes to prepare a quiz or time taking by participants to complete a quiz is still ongoing (Bonneau & Preibusch 2013:258; Cheung & Hew 2009:162). In addition, survey-takers are less satisfied with quizzes as it does not permit flagging questions for later review or changes to their answers (Ganger & Jackson, 2003:5).

Nevertheless, the research question highlighted in this section has been answered affirmatively in section 2.5.3.1, and confirmed by the result of the questionnaire obtained in section 7.4 later analysed in section 8.3. It was not possible to evaluate the effectiveness of the quiz template approach using statistical data since no alternative data collection method was used along with the quiz template in this study. However, using common collection methods such as interviews or observations to gather information from the SN users distributed over the world is difficult and almost impossible (Owoade & Jacob 2013:7). An electronic questionnaire transposed to a quiz template is, therefore, easier to administer and is better attended to by the targeted audience (Rubin & Rubin 2005:23) In addition, the speed at which the respondent welcomed the quiz approach, vis-a-vis the ease of designing and implementing the methodology and data analysis is smooth enough to rank the quiz template approach highest.

9.2.2.6.

Can a technical control that is not based on incident statistics be adequate to measure the effectiveness of awareness in SN?

The findings obtained in section 8.3 identified knowledge, attitude, behaviour/belief, information category, and privacy intentions as the main human determinant factors for a safe SN. The results also suggest that awareness has exclusive controls over users' knowledge only, and not necessarily over other factors. This then implies that no matter how knowledgeable a user is in the area of privacy and security, these other human attributes may render the awareness efforts ineffective.

It therefore follows that an approach that is independent of incident statistics may not, on its own, be adequate to measure the effectiveness of awareness in SN. Awareness could be adequate and sufficient but may not have many impacts on the users and the SNs at large. This proactive approach can only ascertain the adequacy and not necessarily the effectiveness of awareness efforts considering the possible emergence of those other factors that are capable of influencing the research findings. Therefore, just as it is in this research study where both survey and intention-gathering are used to consider the possibility of KAB and users' intention influencing the effectiveness of awareness efforts on the SN (section 7.4), there may be a need for a secondary approach to validate the accuracy and authenticity of the results obtained, and to determine the potential impacts of these aforementioned attributes in the final results.

9.2.3. Summary overview

This section presents an overview of the research questions and answers in a tabular form. It uses table 18 to outline each research question against the respective research response.

Table 18: Research questions vs answers (own compilation)

Question #	Research questions	Research answers
1.	What metrics can be applied to measure online user behaviour in SNs?	Attitude, beliefs, information category, and privacy intentions of users.
2.	What controls are available to measure awareness?	Conventional, unconventional, security metrics and non-incident statistics approach.
3.	Why should technical controls be explored as an option to measure awareness in SNs?	There is a strong need for a proactive approach of measurement.
4.	Can password cracking be used as technical control to measure awareness in SNs?	Yes, password cracking is proactive and does not need to wait for an occurrence of an event or a success of an attack before being used.
5.	Will a quiz template be an appropriate tool for data collection on the SN?	Yes, it will.
6.	Can a technical control that is not based on incident statistics be adequate to measure the effectiveness of awareness in SN?	No. A secondary approach may be required to validate the findings for possible influence of some attributes.

9.3. Technical control – an independent incident statistic approach

The primary question can now be addressed since all six research sub-questions have been answered.

How can technical controls be used to measure the effectiveness of awareness efforts in SNs?

As a synthesis/follow-up to issues identified from the literature reviewed in Chapter 2 and the lapses identified in the existing awareness measurement techniques, a technical control of measurement is introduced to mitigate the challenges. A technical control is the response to the primary research question in this study, since it is implemented as a proactive approach to measure awareness efforts.

This primary research question has been answered along with questions 2, 3, 4 and 6. Although the measurement techniques discussed in section 9.2.2.2 to address question 2 could potentially be applied in measurement of awareness efforts, none of them is preventive and proactive. The need for technical control measures have been addressed in section 9.2.2.3 while attending to question 3, and the responses offered in section 9.2.2.4 to resolve question 4 make it clearer that an independent incident statistics approach of measurement have to be technical and practical. Technical controls can, therefore, be used to measure the effectiveness of awareness efforts in SNs but the output must be validated to eliminate the potential impacts of the influencing factors on the final results (section 9.2.2.6).

9.4. Theoretical contributions

The theoretical contribution of this research is the adaption of the underlying theories, replicating theories, and extending existing models from different fields. This section therefore focuses on the contributions of those theories to the body of knowledge.

9.4.1. Adapting assumptions of underlying theories

This study describes the main referent theories namely system-determined, interaction-determined and people-determined (section 3.3.5) on which the study is based and identifies other unrelated models but practically similar to this study. These models have been discussed in sections 3.3.1 – 3.3.5.

The assumptions underlying systems security and system utilization are *adapted* from these referent theories of system and people's resistance to study the impacts of awareness on SN. The facts in the 'real world' are the themes of this study. The themes are those variables influencing the measurement of awareness efforts in SNs and are grouped into seven (7) categories for the purpose of this study. The first category which is the privacy risks and security threats discussed in section 3.4 is hypothesized as inhibiting factor to privacy and security measurement. The next categories - security techniques (section 6.6) and measurement approaches (sections 3.6 – 3.6.4) - are both hypothesized as enabling factors, while problems in measurement discussed in section 5.5 are inhibiting factors. Other

categories include what to measure (section 5.6), how to measure (section 5.7), and awareness benchmarking and metrics (section 5.8) can be enabling or inhibiting. The influence of some of these attributes on awareness was tested in sections 8.3 and 8.4.

9.4.2. Replicating theories

Theories from other domains, including human behaviour and psychology are replicated in this study and applied to the field of awareness measurement. This work replicates the general concepts adopted in models such as AT, KAB, RCT, TRA and system-determined and people-determined theories, which are technologically applicable and widely accepted.

9.4.3. Extending existing models

This study extends the existing technology assumptions and IS models as follows:

1. Coming from an IS perspective, TRA asserts that factors influencing behaviour of technology users only indirectly do so by influencing subjective norm, attitude or their relative weights. Variables such as information category, privacy intention, and user characteristics also fall into this category. This study however departs from TRA by not relying on the assertion but testing the direct influence of these factors on human insecure behaviour despite the adequacy of awareness as presented in sections 8.4 – 8.6.

2. KAB model submits that knowledge accumulation instigates a change in attitude and behaviour; it principally substantiates the influence of knowledge on people's behaviour, which in turn enforces changes in attitude and behaviour (section 3.3.4). This study disagrees in part with KAB concept by agreeing with Khan et al. (2011:10863) that "a change in user behaviour is not limited to an increase in knowledge alone, as behavioural change is a function of multiple variables". Therefore, while accepting knowledge, attitude, and behaviour (KAB) as the evaluation criteria that determine the effectiveness of awareness on the SNs, findings in Chapter 8 of this study confirmed knowledge as the only indicator of awareness efforts, and, indeed, the only criterion to measure awareness effectiveness since other factors are not necessarily influenced by attitude.

9.5. Methodological reflections and contributions

This section only considers the methodological reflections on the appropriateness of the chosen methodologies and processes of the study. A triangulation approach (section 2.5) is employed in this study since the methodologies used range from quantitative to qualitative. Someone looking at this work from just a pure security perspective may find the methodology too wide

and may argue that data validation, which calls for a qualitative approach, was not necessary since the security metrics identified in section 9.2.2.1 do not necessarily influence awareness efforts on the knowledge of SNs' users.

Nevertheless, the author's position remains that triangulation is the most appropriate to resolve these research problems. As pointed out in section 9.2.2.6, users' knowledge can only be adequate if awareness efforts is sufficient and adequate but the adequacy of users' knowledge does not necessarily make the awareness efforts effective until the influence of the security metrics are put into consideration. A qualitative study of the influence of security metrics on these research findings was therefore absolutely necessary. However, to put all these speculations to rest, issues relating to qualitative and quantitative research methodologies will be reflected on in section 9.5.1, password cracking in section 9.5.2, survey by questionnaire in section 9.5.3, questionnaire design in section 9.5.4, questionnaire administration in section 9.5.5, the data analyses in section 9.5.6, and the development of the SN in section 9.5.7.

9.5.1. Qualitative vs quantitative

While doing this type of research study, it is not unusual that the researcher will confront both social and technical challenges. The literature reviewed were extensive and comprehensive but it is still very possible that past related works, which could have enhanced the author's judgemental positions, are in existence but they are not available or accessible to him. When researching the strength of user passwords, the qualitative approach in the form of observations on the combination of data already aggregated in the password files was indispensable. Although this observation process was automated by a password cracker, it has to be acknowledged that the development of the cracker was influenced by the perception of the research. However, this cannot be an issue to the results obtained after all, "the aim of science is to bring the perceptions as close as possible to the real world" (Van Biljon 2006:218).

This qualitative data-gathering approach was definitely aided by the automation process. This was helpful in understanding the password combinations and classification as guessable or not (section 6.2.2). However, despite that user knowledge is adequate due to sufficient awareness efforts implemented, there is a possibility that some categories of users will stick to insecure behaviour as a result of their attitudes, beliefs, information categories, and privacy intentions (section 8.3 – 8.5), thereby rendering the awareness efforts useless and ineffective in securing SNs. This made the questionnaire (a quantitative research method) an indispensable part of this study as it helped to identify the potential impacts of these control metrics in the research

findings (section 7.3.1), and served as an additional tool to measure the impacts of technical controls and awareness in SNs. Consequently, therefore, going by the response to research question 6 in section 9.2.2.6 and table 18, this study could not have contributed meaningfully to the existing body of knowledge if the qualitative approach was used in isolation.

9.5.2. Password cracking

Following the migration of sOcialistOnline to life, the SN was allowed to be stable at production and made accessible to every user on the internet. The password file was keeping user passwords, and the security file was meant to keep photos and some other related information. The two files were encrypted to ensure data confidentiality.

Password cracking was developed to automate observation processes in the SN. In this study, therefore, it is regarded as a qualitative research approach of cracking the password files and analysing the strength of individual passwords. The number of users using easily guessable passwords is a key indicator of awareness (ENISA 2008:62). Meanwhile, the password cracker only disclosed the security information about each password and not the password combination itself, to give no trace to the participant's identity. This was also done to abide by UNISA's research ethics policy, and to ensure that user data are treated with the adequate privacy and confidentiality.

Typically, SNs do not have a lot of contents when they are newly launched because there will not be many users to generate the content. In the same vein, sOcialistOnline specifically experienced users' low patronage because it was new and not yet popular, thereby necessitating the need to extend the research period to run for 17 months on the internet to be stable enough to generate adequate required primary data. These are users' personal and confidential data, including passwords and photographs. However, the research period could have been extended to 24 months or more for the SN to remain active on the internet and available to the users, so as to gain enough popularity required to gather enough data for analysis.

9.5.3. Survey by questionnaire

This work appreciates the significant differences between a survey by interview and a survey by questionnaire. In either case, a questionnaire can be used as a data-capturing tool, however, in the case of a personal interview the interviewer has the advantage of instantly tailoring his questions in line with the responses (Van Biljon 2006:100). Surveys are quite useful to quantify user preferences and usage but they are not very useful when new needs are to be

discovered (Scandura & Williams 2000:1259). Therefore in measuring the effectiveness of awareness on SN, it is important to understand why some users still use guessable passwords despite their high level of security awareness. This type of information is extremely difficult to capture with interviewing since SN users are scattered all over the world. Questionnaires in the form of quiz templates (section 7.4), are considered to be more suitable for data collection in this research study.

9.5.4. Questionnaire design

No existing questionnaire was found suitable for this study since those available did not focus on the relationship between behaviour, control metrics and awareness of SN users. Hence, a new questionnaire was designed and transposed into a quiz template specifically for this study. This process of developing a new questionnaire is always strenuous and time-consuming; it is indeed an effort whose magnitude was hardly appreciated until towards the end of the study.

Attempts were made to use some questions from existing questionnaires on awareness, but they were not tailored towards SN users. When being adapted for awareness scenarios, the groups of those questions tended to lose their internal validity, and the author had to drop them since it became obvious that they could not be built upon. It was later realised that some of those questions could have been retained to capture time-orientation, location or male/female dimensions which could have tested stronger in influencing awareness efforts on SNs. However, it was more promising that the quantity of the questions were kept at the possible minimum not to dampen the enthusiasm of respondents towards responding to the questionnaire.

Another challenge was that after the quiz had been administered, the author gradually became more aware of some other information that would have been useful to be included in the quiz template. The author believes that, if available, a standardised questionnaire would have addressed this situation. Although some of the open-ended questions were not answered as they call for more personal or mental capability of the respondents, more of these questions ought to have been included in the questionnaire for the survey to cater for more qualitative responses. These may have provided insights to why people still stick to insecure behaviour, and why their intentions and beliefs are not influenced by their good knowledge of awareness.

9.5.5. Quiz administration

The quiz was administered through the web only to users with guessable passwords. Given that participation and attendance were optional and the questionnaires were anonymous as

stated in the second page of the quiz template (Appendix H-ii), the author was not present and he did not have any influence on the entire process. Although follow-up emails were sent to the participants urging them to complete the questionnaire within a stipulated time, it cannot be considered detrimental to the objectivity of the survey.

The quiz was restricted to teenagers and adults since government regulation in some countries (including Nigeria and South Africa) require that the parent of a child give written permission of consent before his/her child can be allowed to complete a questionnaire. This restriction is a blessing in a way to this study as children data were exempted from data gathered since children are fond of giving inappropriate responses to research questions when not properly guided (Cassell & Symon 1994:21).

A web survey was conducted with ease and the turn-around time was considerate, as all the respondents sent in their submissions within seven days of distributing the quiz. However, reviewing the automated time setting that keeps the actual time a respondent take to complete the questionnaire, the web administration did not appear viable. This is because the maximum recommended period to complete a web survey is 10 minutes (Toledano 2005), whereas it took a respondent an average of 17 minutes to complete the questionnaire. A notable challenge here was that not every SN user has free internet access. Hence, access to internet is time-charged (per minutes or hours) and some participants were not ready to spend time and money completing a questionnaire without an incentive attached.

9.5.6. Data analyses

For the reason that triangulation research approach was employed in this study, both descriptive and inferential research statistics were used for data analyses. The author employed inferential statistic to formulate a password analyser using password cracker (observation) to obtaining its input data, while descriptive statistics was used to analyse responses obtained from questionnaire administration (section 2.5.4). The survey samples were then passed through a confirmatory factor analysis.

In this study, the statistical analysis was hindered by limitations of self-reporting. This hindrance was addressed by considering the findings from the password cracker and triangulating those with the quiz or questionnaire. Putting all these into consideration and accepting to live with the limitations, the author believes that the data-gathering and the analyses methodologies were the most appropriate to the research questions.

9.5.7. Development of an SN for this study

For reasons highlighted in sections 1.10.1, a new SN was developed specifically for this study. Although this development approach led to an extended research timeline, collection of primary data for analysis would have been impossible and thereby putting the study to a halt if a dedicated SN was not developed.

The approach gives a good result as the extended timeline did not have any effect on the scientific validity of the study (section 1.10.1). However, researchers seeking to replicate this work should have a flexible timeline to accommodate such delay owing to possible low patronage the newly developed SN may experience.

9.6. Practical contributions

The major contribution of this study to the domain of awareness and SNs is in the design and implementation of the password cracker. These contributions, which make a clear distinction and improvement from the acclaimed existing crackers as previously described, are classified as primary and secondary contributions, and discussed in the next sections.

9.6.1. Primary contributions

Primary contributions are the practical contributions that have to do with the goals and objectives of this study. They include the following:

1. Introduced a proactive approach of measuring awareness efforts in SNs. This is a preventive approach where the effectiveness of the implemented information security is determined before the success of an attack. The password cracker developed for this purpose was tested and implemented acceptably, and the results were verified by control metrics. This approach will be best appreciated especially in industries where the risk tolerance level is very low.
2. Uncovered to the SN owners, the prospect of using technical controls as information security measures and not only to secure information. The literatures reviewed in sections 3.4 – 3.6 confirm that all the technical controls postulated by each of the authors have always been tailored towards tightening information security. None was on awareness measurement, including privacy watch by Esma et al. (2010) and API by Asim et al (2010).
3. Invented a new password cracker with a genuine motive of awareness measurement. This may be made available to other authors interested in this area of study. The existing crackers (table 11) as asserted by some vendors are mainly to crack passwords for hidden

agendas. Even with that, their potency is in doubt as their claims on which their solution is based, that most popular SNs hash their password files with MD5, have been faulted (section 7.2).

4. Web quiz deployed in this research is presented to the future researchers as a verification tool to influence security dimensions on awareness efforts. It was demonstrated that technical controls will be more effective in measuring the effectiveness of awareness techniques when the influence of security dimensions on the result obtained are taken into consideration. The web quiz was adjudged effective in the administering questionnaire that generated the input data used to determine the impacts on the user knowledge, attitude, behaviour, and information category.
5. Identified users' sharing intentions and their impacts on awareness efforts. The table of information category (table 14) could be adopted by a future author for a similar investigation, while various sharing intentions of users are being recognised as major factors behind the effectiveness of awareness efforts in SNs.
6. Postulated control metrics that influence awareness efforts. These are not measurement methods or approaches but factors that determine the effectiveness of awareness efforts no matter how sufficient or adequate the effort is. Awareness evaluators need not to rely on users' knowledge again but attitude, beliefs, information category, and privacy intentions of users to ascertain the impacts of awareness on SNs.

9.6.2. Secondary contributions

In the course of this study, some potential problems were uncovered, which had to be addressed for the continuity of this research. These solutions, which are considered significant and are regarded as the secondary contributions to the scientific body of knowledge, are as follows.

1. A safe SN – sOcialistOnline – is invented that, when finally polished and publicised, may compete favourably with the popular sites like Facebook and Twitter, and be a preferred SN to the users. The author had no option than to come up with a safe SN since gaining administrative access to the established SNs was not possible as organisations feel unsafe and over researched.
2. A standardised questionnaire for present and future use is produced. As pointed out in the data gathering stage (section 7.3.2), it was not possible to get a suitable questionnaire to capture awareness contents of SN users that include normative beliefs and habits since the ones available are more specific on certain issues like user knowledge or beliefs, but not

both. The author had to refine some of these questions, before being updated and tested. The final questionnaire produced is more refined and of a wider scope and may be useful for scholars in a similar field to measure control metrics, normative beliefs and users' sharing intentions.

3. This study promoted the arguments in favour of security investment moving from a technology operation-based to a risk analysis and mitigation philosophy. While this may not be considered as a new debate as such, the emphasis in this study has enhanced the cost-benefit analysis justification to the SNs and other business owners on funding the risks prevention and mitigation.

9.7. Recommendations for future work

"Research is a quest for answers to a problem stimulated by a curiosity or interest, which leads to the researcher embarking on a journey of many paths fraught with unknowns to discover truths and eventually arrive at answers, new knowledge, and fresh insights while uncovering new questions, thereby continuing the cycle of knowledge creation and evaluation" (Padayachee 2013:315). Going by this definition therefore, the under-listed are considered as further research opportunities emerged during the course of this study.

1. The implementation of sOcialistOnline is platform-independent and it is not limited to a particular environment. However, 95% of the SN users in this study are students, making the study academic to an extent. An enhanced implementation of this solution is required to attract adequate research data from other platforms for comparative analysis.
2. Evaluation criteria to measure the impacts of SN providers on awareness efforts have long been discovered, and the ones for user behaviour have also been established in section 8.6 of this study. However, there is a need for future authors to identify those evaluation criteria to measure the impact of third-party applications on awareness efforts in SNs.
3. SNs should emulate the awareness efforts implemented in this study, and much more to raise user awareness to the maximum. Rather than terms and conditions, user-friendly community guidelines should always be published on the sites to educate users in real-time. Accessible and refined languages are also required to enhance user understanding and compliance to the SN's regulations.
4. As established in this study, awareness efforts have absolute control on user knowledge but not necessarily on the control metrics (habit, attitude, intention, and behaviour). Since control metrics are deterrents to awareness efforts, future work is required in this area to put these metrics under controls.

5. As highlighted in section 5.7.3, several security measurement metrics have been identified by previous authors. Apart from being incident statistics, they are all knowledge-based implying that they can only be adequate, not necessarily efficient for awareness measurement (sections 8.3 and 9.2.2.1). Further research on these metrics is thereby recommended to establish their efficiency of measurement.
6. A research into the application of the measurement approach that is independent of incident statistics as presented in this study to other areas of interest such as knowledge management systems (KMS) is required to ascertain the portability of the technique to several platforms.

9.8. Conclusion

Awareness is important but the measurement of its efforts in SNs is of more significance to this study. As pointed out in literature review, past related works of awareness on SNs have mostly failed to make provision for data validation (ABC 2013:9). Rather, they only succeeded in producing awareness measurement techniques – incident statistics approaches – driven by occurrence of an event or success of an attack. This work addressed some of these limitations by introducing to the SN's owners a password cracker that does not only alert the users of their password strength but can also be used to measure the impact of awareness efforts on SNs.

Password crackers have been built onto some email applications recently but according to the literature reviewed so far, none has ever been successfully applied to an SN. The recent claims by some password stealers and crackers (e.g. Pendriveapps 2013, OnlineHashCrack 2013, Stock & Barto 2013) to crack Facebook are just mere speculations as the basis of their justifications of Facebook using MD5 for password hashing is faulty (section 7.2). Even in applications where password crackers are built-in, these crackers are only used as control measures and not as measures of control efforts. That is, they are being applied to secure applications and not necessarily to measure the impacts of awareness efforts. This is where this study makes a major difference as the research is targeted at producing a technique that is independent of incident statistics but proactive and efficient enough for the practitioners to measure the effectiveness of awareness in SNs.

This password cracker developed in response to the research question: "How can technical controls be used to measure the effectiveness of awareness efforts in SNs?" The cracker is structured in sOcialistOnline in such a way to screen prompt users about the weaknesses in their password combinations at the account set-up, thereby raising awareness amongst SN's users. The strength analysis of the individual password combination is reviewed further to

generate a security strength report used by the SN's owners to measure the impacts of various awareness techniques implemented on the SN.

Based on the definition offered in section 1.2, password cracker scanner meet the criteria for technical controls to the extent that they were implemented as an approach independent of incident statistics to measure the effectiveness of awareness techniques within the scope of this study. This author, therefore, presents this solution to the body of knowledge on the condition that it should not be used in isolation for reasons emphasised in section 9.2.2.6.

REFERENCES

ABC (2013). Measuring Information Security Awareness Techniques; the Pros and the Coins. ABC Nig. Press, University of Maiduguri, Nigeria.

Adams, A and Sasse, M (1999). Users are not the enemy. Communications of the ACM 42(12), pp 41-46.

Adebesin, T.F. (2011). Usability and Accessability Evaluation of Digital Doorway. MSc. Thesis, Department of Information Systems, University of South Africa (UNISA).

Administrator (2012). Creating an Social Networking Site Like Facebook. Advanced PHP Solution. Available Online: http://advancedphpsolutions.com/blog/social-networking/create-a-social-networking-site-like-facebook/. Date Retrieved: February 9, 2013.

Aiello, L.M and Ruffo, G. (2011). Tunable Privacy to Distributed Online SN Services. Computer Communication, doi:10.1016/j.comcom.2010.12.006. Date Retrieved: June 2, 2003.

AirlineLeader (2011). The Airline CEO's Guide to SN and the new Customers' Relation Paradigm. Available online: http://www.airlineleader.com/CustomContentRetrieve.aspx?ID=1387612&A=SearchResult&SearchID=122739&ObjectID=1387612&ObjectType=35. Date retrieved: May 15, 2011.

Al-Awadi, M. A. (2009). A Study of Employee's Attitudes Towards Organisational Information Security Policies in the U.K. and Oman. Ph.D. Dissertation, Department of Computing Science, Faculty of Information and Mathematical Sciences, University of Glasgow.

Albert, S. (2008). How Airlines are Using Social Media. Available online: http://www.dirjournal.com/articles/airlines-social-media/. Date retrieved: September 18, 2011

Albrechsten E. and Hovden J. (2010). Improving Information Security Awareness and Behavior Through Dialogue, Participation, and Collective Reflection. An Intervention Study. Journal of Computer Security, 29(4): 432-445.

Asim, S.I., Mehmet, E.Y. & Abdul H.Z. (2010). An Approach for Protecting Privacy on SNs. 2010 Fifth International Conference on Systems and Networks Communication. Date Retrieved: June 12, 2011. Available online: http://www.academia.edu/941420/an_approach_ for_ protecting_privacy_on_social_networks. Date Retrieved: October 29, 2012.

Bace, R and Mell, P. (2001). NIST Special Publication on Intrusion Detection Systems. National Institute of Science and Technology incorporated Booz and Hamilton Inc. McLean VA. Available online: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix= html&identifier=ADA393326. Date Retrieved: August 22, 2014.

Bangkok (2010). Today's 10 Most Common Security Threats on The Net. Bangkok Pest Teck. Available online: http://www.bangkokpost.com/tech/computer/34952/today-10-most-common-security-threats-on-the-net. Date Retrieved: January 20, 2013.

Barry (2012). The Case for Security Awareness. Security and Coffee. Available online: http://securityandcoffee.blogspot.com/2012/08/the-case-for-security-awareness.html. Date Retrieved: November 29, 2013.

Bell, T. (2010). The Social Psychology of IT Security Auditing from the Auditee's Vantage Point: Avoiding Cognitive Dissonance. ISACA Journal, Vol. 3, 2010. Available online: http://www.isaca.org/Journal/Past-Issues/2010/Volume-3/Pages/The-Social-Psychology-of-IT-Security-Auditing-From-the-Auditees-Vantage-Point.aspx. Date Retrieved: January 28, 2013.

BIS (2009). Information Technology-Security Techniques-Management of Information and Communication Technology Security, IS/ISO/IEC 13335-1:2004 Part 1; Concepts and Models.

Bond, T (2012). Employee Security Awareness Survey. Trend Bond. SANS Education, version 1.3. Available online: http://www.sans.edu/student-files/awareness/employee-security-awareness-survey.pdf. Date Retrieved: January 29, 2013.

Bonneau, J. and Preibusch, S. (2013). The Privacy Jungle: on the Market for Data Protection in SNs. The Eighth Workshop on the Economics of Information Security, Greece, pp. 250-261. Available online: http://weis09.infosecon.net/files/156/index.html. Date Retrieved: June 14, 2014.

Boss, S. R. (2007). Controls, Perceived Risk and IS Precautions: External and Internal Motivations for Security Behaviour. Ph.D. Dissertation, University of Pittsburgh, Pennsylvania.

Boyd, D. (2007). SN: Public, Private, or What? The Knowledge Tree: An E-Journal of Learning Innovation. Available online: http://kt.flexiblelearning.net.au/tkt2007/?page_id=28. Date Retrieved: July 23, 2011.

BR (2005). Committed to Protecting America: CEO Guides to Security Challenges. Business Roundtable. Available online: http://www.cj.msu.edu/~outreach/wmd/ceo_guide.pdf. Date Retrieved: May 29, 2013.

Brace, I. (2004). Questionnaire Designs: how to plan, Structure and Write Survey Materials for Effective Market Research (1st ed.). London: Sage Publications.

Briggs, L. (2009). Locking Down Data at U Nebraska. Available online: http://campustechnology. com/articles/2009/10/15/locking-down-data-at-u-nebraska.aspx. Date Retrieved: July 23, 2011.

Brodie, C. (2009). The Importance of Security Awareness Training. SANS Infosec Reading Room. Available online: http://www.sans.org/reading_room/whitepapers/awareness/importance-security-awareness-training_33013. Date Retrieved: May 23, 2011.

Bulgurcu, B. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS quarterly special issue, 34(3), 523-548. Available online: http://www.academia.edu/3059288/Information_Security_Policy_Compliance_An_Empirical_Study_of_Rationality-Based_Beliefs_and_Information_Security_Awareness. Date Retrieved: September 13, 2014.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2009). Effects of Individual and Organisation Based Beliefs and the Moderating Role of Work Experience on Insiders' Good Security Behaviours. 2009 Proceedings of IEEE Workshop on Software Security Process, August 29-31. Vancouver, Canada.

Carr, L. T. (1994). The Strengths and Weaknesses of Quantitative and Qualitative Research: What Method for Nursing? Journal of Advanced Nursing, 20 (4):716-721.

Cassell, C. and Symon, G. (1994). Qualitative Methods in Organisational Research. Thousand Oaks, CA: Sage Publications.

Chan, Y. and Wei, V. (2009). Teaching for Conceptual Chance in Security Awareness: A Case Study in Higher Education. IEEE Security and Privacy, 7(1), 68-71, 2009.

Chapple Mike (2005). Four Ways o Measure Security Success. Information Security Magazine. Available online: http://searchsecurity.techtarget.com/tip/Four-ways-to-measure-security-success. Date Retrieved: October 28, 2012.

Cheung, W.S and Hew, K.F. (2009). A Review of Research Methodologies Used in Studies on Mobile Handheld Devices in K-12 and Higher Education Settings. Nanyang Technological University, Australasian Journal of Education Technology 25(2):153-183. Available online: http://www.ascilite.org.au/ajet/ajet25/cheung.pdf. Date Retrieved: September 19, 2013.

Cheng, L. (2009). Thinking about Thinking: Relative Value Vs Absolute Values. The Philosophy Pop Culture. Available online: http://larrycheng.com/2009/06/24/relative-value-v-absolute-value/. Date Retrieved: November 12, 2013.

Chizomadia, D (2012). Using the principle of Least Authority to Improve Software Assurance. Promia Inc., Senior Software Assurance Architect. Available online: http://www.omg.org/news/meetings/workshops/SWA_2007_Presentations/05-2_Chizmadia.pdf. Date Retrieved: September 15, 20013.

Ciccone, D. (2009). Facebook Connect Fully Integrated Into Mobility Today. Mobility Today Fitness. Available Online: http://web.archive.org/web/20101024033731/http://mobilitytoday.com /news/009500/facebook_connect_mt. Date Retrieved: September 10, 2012.

CISC (2010). Criminal Intelligence Service Canada. 2010 Reports on Organised Crime. Available online: http://www.cisc.gc.ca/annual_reports/annual_report_2010/document/report _oc_2010_e.pdf Date Retrieved: January 12, 2013.

Collins, I. (2010). 5 Common Uses of Social Networking and the Effect on Your Target Audience. Blogussion Skin, Premium WordPress Theme. Available online: http://www.blogussion.com/general/uses-social-networking/. Date Retrieved: April 3, 2013.

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

Continuity C. (2006). UK Government Biennial Information Security Breaches Survey Published. Continuity Central, Infosecurity Europe, London. Available online: http://continuitycentral.com/news02393.htm. Date retrieved: January 25, 2012.

Convertino, M., Baker, K.M., Vogel, J.T., Suedel, B. (2013). Multi-criteria Decision Analysis to Select Metrics for Design and Monitoring of Sustainable Ecosystem Restorations. Ecological Indicators Elsevier Journal. Available online: http://digitalcommons.unl.edu/cgi/viewcontent.cgi? article=1189&context=usarmyresearch. Date Retrieved: November 12, 2013.

Creswell, J. W. (2003). Research Design: Qualitative, Quantitative and Mixed Method Approaches. Thousand Oaks, CA: Stage Publications.

CSI (2006). Virus Attacks Named Leading Culprit of Financial Loss by U.S.A. Companies in 2006 CSI/FBI Computer Crime and Security Survey. Available Online: http://www.gocsi.com/press/20060712.jhtml. Date Retrieved: March 4, 2012.

CSI (2007). The 12th Annual Computer Crime and Security Survey. Available Online: http://www.gocsi.com/forms/csi_survey.jhtml. Date Retrieved: April 14, 2012.

Day, S. (2013). Self-Disclosure on Facebook: How Much do we Really Disclose? Journal of Applied Computing and Information Technology, 17(1). Available online: http:// www.citrenz.ac.nz/jacit/JACIT1701/2013Day_Facebook.html. Date Retrieved: July 19, 2013.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. (3rd e, Ed.) MIS Quarterly, 13(3), 319–340.

Davis, P. (2008). Measuring The Effectiveness of IS Awareness Training. - Whitepaper Sai Global. Available Online: http://www.oceg.org/view/measuring-the-effectiveness-of information-securit. Date Retrieved: March 17, 2011.

Deborah, J. B. and Richard G. (2011). Cyber Resiliency Engineering Framework. MITRE Technical Report, the MITRE Corporation, Bedford, MA. Available Online: http://www.mitre.org/work/tech_papers/2012/11_4436/11_4436.pdf. Date Retrieved June 1, 2012.

Dionysiou, I. (2012). Security is in The eye of the Beholder: Security Perceptions and Challenges in SNs. ICIW 2012: Seventh International Conference on Internet and Web Applications and Services. Available online: http://www.thinkmind.org/index.php?view= article&articleid=iciw _2012_5_30_20116. Date Retrieved: December 2, 2013.

Dowling, C. D. (2009). Internal Data Protection and Privacy Law. White and Case. Available Online: http://www.whitecase.com/files/publication/367982f8-6dc9-478e-Ab2f-5fdf2d96f84a/ presentation/publicationattachment/30c48c85-A6c4-4c37-84bd-6a4851f87a77/Article_ intldataprotectionandprivacylaw_V5.Pdf. Date Retrieved: September 28, 2012.

Duffy, T. (2010). Nine Steps to Creating a Social Networking Site That Kills Facebook. TECHi.com. Available online: http://www.techi.com/2010/06/9-steps-to-creating-a-social-networking-site-that-kills-facebook/. Date Retrieved: February 9, 2013.

Melancon, D. (2012). Security Metrics: What are you Measuring? The State of Security. Available online: http://www.tripwire.com/state-of-security/security-data-protection/security-metrics-what-are-you-measuring/. Date Retrieved: November 12, 2013.

Endicott-Popvsky, B., Orton, I., Bailey, K. and Frincke, D. (2005). Community Security Awareness Training. Proceedings of the 2005 IEEE Workshop on Information Assurance and Security, New York, 373-379.

Engestrom, Y. (1987). Learning by expanding: an activity-theoretical approach to developmental research. Helsinki: Orienta-Konsultit.

Engestrom, Y. (2001). Expansive learning at work: toward an activity theoretical reconceptualization. Journal of Education and Work, 14(1):133-156.

ENISA (2007). Information Security Awareness Initiatives: Current Practice and Measurement of Success. Available Online: http://www.itu.int/osg/csd/cyber-security/WSIS/3rd_meeting_ docs/contributions/enisa_measuring_awareness_final.pdf. Date Retrieved: May 18, 2011.

ENISA (2008). The new User's Guide: How to Raise IS Awareness. Available Online: http://www. ENISA.europa.eu/act/ar/deliverables/2008/new-users-guide. Date Retrieved: December 12, 2011.

ENISA, (2010). The New User's Guide: how to Raise IS Awareness. Available Online: http://www. ENISA.europa.eu/act/ar/deliverables/2010/new-users-guide. Date Retrieved: December 4, 2011.

EPIC (2008). Facebook Privacy Page. Available Online: http://epic.org/privacy/facebook/ default.html. Date Retrieved: June 7, 2011.

Ernst and Young (2004). Global IS Survey 2004. Available Online: http://www.ey.com/global/download.nsf/uk%20survey_global_information_security_04/$file/ey_giss_%202004_eyg.pdf. Date Retrieved: June 4 2012.

Esma, A., Sebasten, G. and Ai, Ho (2010). Towards a Privacy-Enhanced Social Networking Site. 2010 International Conference on Availability, Reliability and Security. Available online:

http://www.mendeley.com/research/towards-privacyenhanced-social-networking-site-17/. Date retrieved: June 7, 2011.

Facebook (2013). Who can see Stories About my Comments and Likes in News Feed and Ticker? Facebook. Available online: https://www.facebook.com/help/www/171783462899295. Date retrieved: October 25, 2013.

Farrior M (2005). Breakthrough Strategies for Engaging the Public: Emerging Trends in Communications and Social Sciences. Biodiversity project. Available online: https://www.comminit.com/en/node/223510/306. Date Retrieved: January 27, 2013.

Field, A. (2005). Discovering Statistics Using SPSS (2nd ed.). London: Sage Publications.

Fishbein M. and Ajzen I. (1975). Belief, Attitude, Intention and Behavior: an Introduction to Theory and Research. Reading, MA, Addison-Wesley.

Forget, A, Chiasson, S., Van Oorschot, P., and Biddle, R. (2008). Improving Text Passwords Through Persuasion. Symposium on Usable Privacy and Security (SOUPS'08). Pittsburgh, PA, U.S.A.

Fryer, D. (1991). Qualitative Methods in Occupational Psychology: Reflections Upon why They are so Useful but so Little Used. The Occupational Psychologist, (Special Issue on Qualitative Methods), 14:3-6.

FTC (2010). Twitter Settles Charges That it Failed to Protect Consumers' Personal Information, Federal Trade Commission (FTC). Available Online: http://www.ftc.gov/opa/2010/06/twitter.shtm. Date Retrieved: May 25, 2011.

Fulford, H. and Doherty, N.F. (2003). The effects of Culture on Performance Achieved Through the use of Human Computer Interaction. Proceedings of SAICSIT, pp. 218-230.

Ganger, A. C. and Jackson, M. (2003). Wireless Handheld Computers in the Preclinical Undergraduate Curriculum. Medical Education Online, 8(3). Available online: http://www.med-edonline.org/pdf/t0000031.pdf. Date Retrieved: August 5, 2013.

Gartner (2011). User Awareness in SNing. Available Online: http://www.gartner.com/ research/spotlight/asset_118887_ 895.jsp. Date Retrieved: April 1, 2012.

Geary, J. (2011). Privacy and Social Media Investigation: How I Tracked Down an Entire Family From one Tweet. Available Online: http://www.joannageary.com/2011/08/02/privacy-and-social-media-investigation-how-I-tracked-down-an-entire-family-from-one-tweet/. Date Retrieved: February 7, 2012.

Giles, H. (2007). Security Issues and Recommendations for Online SNs. ENISA Position Paper #1. Available Online: http://www.ENISA.europa.eu/act/res/other-areas/social-networks/ security-issues-and-recommendations-for-online-social-networks- Date Retrieved: May 2, 2011.

Glynn, F. (2014). What is Vulnerability Assessment and Penetration Testing (VAPT)? Vulnerability Assessment and Penetration Testing, VERACODE Software Security Testing. Available online: http://www.veracode.com/security/vulnerability-assessment-and-penetration-testing., Date Retrieved: August 22, 2014.

Gross, R., Acquisti, A., and Heinz, H.J. (2005). Information Revelation and Privacy in Online SNs. Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, Alexandria, U.S.A. Date Retrieved: July 24 2012.

Guenther, M. (2001). Melissa Guenther, LLC. Available online: http://www.iwar.org.uk/comsec/resources/sa-tools/Security-Awareness-Quiz-Questions.pdf. Date Retrieved: February 27, 2013.

Hagen, J. Albrechtsen, E. and Hovden, J. (2008). Implementation and Effectiveness of Organisational Information Security Measures. Information Manage. Computer Security, 16(4):377-397.

Hashim, N.H. and Jones, M.L. (2007). Activity Theory: A framework for qualitative analysis. Research online, 4th international Quality Research Convention (QRC), Hilton, Malaysia. Available online: http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1434&context= commpapers. Date Retrieved: September 14, 2014.

Hassan, M.R. and Hussin, H. (2010). Self-Awareness Before Social Networking: Exploring the User Behaviour and Information Security Vulnerability in Malaysia. Proceeding of 3rd International Conference on ICT4M 2010.

Heidari, H. (2010). Design Patterns and Refactoring for Security in Social Networking Applications, Multimedia University, Malaysia. Available Online: http://www.kaspersky.com/se-asia-it-security-conference. Date Retrieved: July 15, 2011.

Helpnetsecurity (2010). 100 Million Facebook Pages Published on Torrent Site. Available Online: http://www.net-security.org/secworld.php?id=9652 Date Retrieved: July 25, 2011.

Hendrickson, M. (2007). Nine Ways to Build Your own SNs. TechCrunch. Available online: http://techcrunch.com/2007/07/24/9-ways-to-build-your-own-social-network/. Date Retrieved: February 12, 2013.

Herzog P. (2006). Open-Source Security Testing Methodology Manual (OSSTMM), Institute for security and open methodologies (ISECOM). Available online: https://www.sos.state.co.us/pubs/elections/VotingSystems/files/OSSTMM-2-2.pdf. Date Reviewed: August 23, 2014.

Hinson, G. (2006). Seven Myths About IS Metrics. Noticebored. Available Online: http://www.noticebored.com/IsecT_paper_on_7_myths_of_infosec_metrics.pdf. Date Retrieved: February 9, 2011.

Hinson, G. (2012). The True Value Of IS Awareness. Noticebored. Available Online: http://www.noticebored.com/html/why_awareness_.html. Date Retrieved: August 23, 2011.

Hollnagel, E. Woods, D.D., and Leveson, N. (2006). Resilience Engineering: Concepts and Precepts Ashgate, Aldershot, UK, 410pg.

Holtzblatt, K. and Beyer, H. (2005). Notes on Contextual Designs. Bjoern Publishers Inc., Morgan Kaufmann, ISBN:1558604111.

Hopper, E., (2010). Intelligent Strategies and Techniques for Effective Cyber-Security, Infrastructure Protection and Privacy. The 5th International Conference for Internet Technology and Secured Transactions (ICITST-2010), London, UK, 2010.

Huffposttech (2011). Facebook Tops Google as Most Visited Website of the Year. Available Online: http://www.huffingtonpost.com/2010/12/30/facebook-tops-google-as-m_n_802606.html. Date Retrieved: July 23, 2011.

Hyland, P. N. (1998). Exploring some problems in information retrieval: an activity theory (AT) approach. Information systems and Activity Theory: Tools in Context. Wollongong: University of Wollongong Press. pp. 93-108.

Info (2011a): A regulatory Compliance: United States Data Federal and State Privacy Laws. Available On line: http://www.informationshield.com/usprivacylaws.html. Date Retrieved: March 5 2012.

Info (2011b): Regulatory Compliance: International Privacy Laws. Available Online: http://www.informationshield.com/intprivacylaws.html. Date Retrieved: June 18 2011.

Infosecurity (2012). Information Security Breaches Survey – Technical Report. Department for Business Innovation and Skills, U.K. Available online: http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf. Date Retrieved: August 30, 2013.

ISAl (2010). The Financial Management of Cyber Risks: An Implementation Framework for CFOs. American National Standard Institute (ANSI), Published By ANSI. Available Online: http://www.isaca.org/chapters2/new-york-metropolitan/membership/ Documents/2011-12-15%20Adams%204.Pdf. Date Retrieved: December 4 2011.

ISF (2005). The Standard of Good Practice for Information Security. Information Security Forum. Available online: http://www.securitymanagement.com/archive/library/isf_tech0505.pdf. Date Retrieved: January 18, 2013.

ITU-T (2003). Security in Telecommunication and Information Technology: An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications, Telecommunication Standardisation Sector of International Telecommunications Union (ITU), Geneva. Date Retrieved: July 24, 2014.

IWS (2007). DOD Information Systems Security Awareness CBT, Computer and IS. Available Online: http://www.iwar.org.uk/comsec/resources/sa-tools/index.htm. Date Retrieved: June 4 2012.

Iyer, A. (2009). Are Facebook's Privacy Settings Working? Available online: http://www.artificialignorance.net/blog/facebook/arefacebooks-privacy-settings-working/. Date Retrieved: December 29, 2012.

Jagatic, TN., Johnson, M., Jakobsson, M., Menczer, F. (2007). Social Phishing. Communications of the ACM, Vol. 50(10), 19-27.

Jithin, A.J. (2012). Is A Facebook Account Essential? Ji-Make Web Services. Available online: http://jimake.blogspot.com/2012/05/is-facebook-account-essential.html. Date Retrieved: June 2, 2012.

Johnson, A. (2012). SN Settings are Ineffective. Information and Communication Journal, Department of Computer Sciences, University of Lagos, Nigeria, Vol. 12(3):27-41.

Johnston, M. (2013). Critic's Choice for Best SN Software. CMS Critic. Available online: http://www.cmscritic.com/PhPFox -review/. Date Retrieved: July 28, 2013.

Jones, H and Soltren, J.H. (2005). Facebook: Threats to Privacy. Project MAC: MIT Project on Mathematics and Computing 2005. Available online: http://groups.csail.mit.edu/mac/ classes/6.805/student-papers/fall05-papers/facebook.pdf. Date Retrieved: November 29, 2013.

Judge, P. (2011). 2011 Social Network Security and Privacy. Barracusalabs Networks Inc. Available Online: http://www.barracudalabs.com/snsreport/2011socialnetworkingstudy.pdf. Date Retrieved: February 3, 2012.

Kabay, M.E. (1993). Social Psychology and INFOSEC. The Risks Digest: Forum on Risks to the Public in Computers and Related Systems, Vol. 15(16). Available Online: http://catless.ncl.ac.uk/risks/15.16.html#subj1. Date Retrieved: February 7, 2012.

Kaptelinin, V. (2013). Activity Theory: How to cite in your report. Interaction Design Foundation, the Encyclopaedia of Human-Computer Interaction. Available online: http://www.interaction-design.org/encyclopedia/activity_theory.html. Date Retrieved September 14 2014.

Kelleher, J. (1984). An Empirical Analysis of Security Awareness Among Data Processing Professionals. Unpublished Master's Thesis, University of San Diego, San Diego, California, U.S.A.

Khan, B, Alghathbar, K.S., Nabi, S.I., and Khan, M.K. (2011). Effectiveness of Information Security Awareness Methods Based on Psychological Theories. African Journal of Business Management Vol. 5(26). Available online: http://www.academicjournals.org/article/article1380536009_ Khan%20et%20al.pdf. Date retrieved: October 27, 2012.

Kiesow, D. (2011). Facebook, Most Visited Website of 2010, Valued At $50 Billion. Pointer. Available Online: http://www.poynter.org/latest-news/media-lab/social-media/112651/facebook-most-visited-website-of-2010-valued-at-50-billion/. Date Retrieved: July 23, 2011.

Kolb, N. and Abdullah, F. (2009). Developing an Information Security Awareness Programme for a Non-Profit Organisation. International Management Review, 5(2):102-108.

Koremans S. (2010). Who is the Biggest Threats to Business Security? Staff or Cyber Criminals. Technology Switched on, News.Co.Au. Available Online: http://www.news.com.au/technology/biz/whos-the-biggest-threat-to-business-security-staff-or-cyber-criminals/story-fn5lic6c-1225871527070. Date Retrieved: July 23, 2011.

Kramer, F. (2012). The Importance of Social Media for Business. Farrel Krammer Communications. Available online: http://www.farrellkramer.com/blog/bid/137032/The-Importance-of-Social-Media-for-Business. Date Retrieved: January 12, 2013.

Kruger, H. and Kearney, A. (2005). Measuring IS Awareness: A West Africa Gold Mining Environment Case Study. A Proceedings of ISSA, Pretoria, South Africa. Available online: http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/018_Article.pdf. Date Retrieved: July 25, 2011.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J. and Nunge, E. (2007). Protecting People From Phishing: the Design and Evaluation of an Embedded Training E-mail System. Conference on Human Factors in Computing Systems Archive. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. San Jose, California, U.S.A., 2007, pp. 905 – 914.

Kyle, A.H. (2011). Top 10 Most Visited Website of 2011. Kaleazy Creative. Available online: http://kaleazy.com/top-10-most-visited-websites-of-2011. Date Retrieved: July 23, 2011.

Lacey, D. (2009). Managing the Human Factor in Information Security: How to win Over Staff and Influence Business Managers. Wiley, John and Sons, Incorporated: Hoboken, New Jersey, ISBN: 0470721995, ISBN-13: 9780470721995, 384 pages.

Leach, J. (2003). Improving User Security Behaviour. Computers and Security, Vol. 22 (8):652-737.

Larson, S. (2013). Facebook Just Killed a Privacy Setting, so It's a Good Time to do Your own Checkup. Available online: http://readwrite.com/2013/10/10/facebook-privacy-setting-checkup#awesm=~onyTNn8KpHCURX. Date Retrieved: November 18, 2013.

Lessin, S. (2012). Better Controls for Managing Your Content. Facebook Newsroom. Available online: http://newsroom.fb.com/News/547/Better-Controls-for-Managing-Your-Content. Date Retrieved: November 18, 2013.

Lindstrom, P. (2012). Security: Measuring up. IS Magazine. Available online: http://searchsecurity.techtarget.com/tip/security-measuring-up. Date Retrieved: June 21 2011.

Lspitzner (2010). Security Awareness Metrics. SANS, Securing the Human. Available online: http://www.securingthehuman.org/blog/2010/04/14/metrics. Date Retrieved: September 23, 2011.

Lucas, M. and Borisov, N. (2008). Flybynight: Mitigating the Privacy Risks of SNing. Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society, pp 1-8, ACM New York, NY, U.S.A.

Madejski, M., Johnson, M., and Bellovin, S.M. (2011). The Failure of Online SN Privacy Settings. Columbia University Press. Available online: http://www.futureofprivacy.org/wp-content/uploads/2011/07/the%20failure%20of%20online%20social%20network%20privacy%20settings.pdf. Date Retrieved: May 3, 2013.

Manly, C. (2013). IT Security Awareness Survey. Library System, Cornell University Library Information Technologies. Available online: https://cornell.qualtrics.com/SE/?SID=SV_1Xs2GRV6rWl88Xr. Date Retrieved: November 27, 2013.

Marks, A. and Rezgui, Y. (2009). A Comparative Study of Information Security Awareness in Higher Education Based on the concept of Design Theorising. International Conference on Management and Service Science, Wuhan.

Mataracioglu, T. and Ozkan, S. (2010). User Awareness Measurement through Social Engineering. International Journal of Managing Value and Supply Chains (IJMVSC) Vol. 1, No. 2. Available online: http://airccse.org/journal/mvsc/papers/1210ijmvsc02.pdf. Date Retrieved: July 24, 2011.

McCarthy, B. (2002). New Economics of Sociological Criminology, Annual Review of Sociology, 28(1), 417-442.

McCoy, C. and Fowler, R.T. (2004). You are the key to Security: Establishing a Successful Security Awareness Programme. The Proceedings of the SIGUCCS'04, Baltimore, Maryland, October 10-13, 2004. Date Retrieved: April 1, 2012.

McNeil, A (2012). How Facebook Beat MySpace. Investopedia US, a division of ValueClick Inc. Available online: http://www.investopedia.com/financial-edge/0212/how-facebook-beat-myspace.aspx Date Retrieved: December 8, 2013.

Meister, E. and Biermann, E. (2008). Implementation of a Socially Engineered Worm to Increase IS Awareness. Third International Conference on Broadband Communications, Information Technology and Biomedical Applications, Gauteng. IEE Computer Society, page 343-350.

MindTools (2013). The Ladder of Inference: Avoiding Jumping to Conclusions. MindTools Essential. Available online: http://www.mindtools.com/pages/article/newTMC_91.htm. Date Retrieved: November 12, 2013.

Mitchamz, Z.S. (2013). Security Awareness Metrics – Informal Survey by HEISC. EDUCAUSE. Available online: http://preview.tinyurl.com/awarenessmetrics. Date Retrieved: May 27, 2013.

Mouton, J. (2001). How to Succeed in Master's and Doctoral Studies. Pretoria. Van Schaik Production.

Myers, M.D., and Avison, D. (2002). Qualitative Research in Information Systems: a reader. (Michael D. Myers and David Avison., Ed.). London: Sage Publications, pp 1-312.

Myers, M.D. (2013). Qualitative Research in Business and Management. Illustrated/Revised edition, ISBN 0857029738, 9780857029737. London: Sage Publications, pp 1-296.

Nagy, J. and Pecho, P. (2009). SNs Security. The Third International Conference on Emerging Security Information, Systems and Technologies, Anthens, 2009, pp. 321-325.

Native I. (2012a). Security Awareness Metrics; Measure What Matters. Native Intelligence Inc., IS Awareness Courses, Posters, Daily Tips. Available online: http://www.nativeintelligence.com/ni-programmes/metrics-03.asp. Date Retrieved: September 15, 2012.

Native I. (2012b). Security Awareness Metrics; Measure What Matters. Native Intelligence Inc., IS Awareness Courses, Posters, Daily Tips. Available online: http://www.nativeintelligence.com/ni-programmes/metrics-01.asp. Date Retrieved: August 3, 2012.

NCSA (2006). National Cyber-Security Alliance. CA/NCSA Social Networking Cyber-Security-Survey. Available online. http://staysafeonline.org/features/SocialNetworkingReport.ppt. Date Retrieved: June 15, 2013.

Nyabando, C. J. (2008). An Analysis of Perceived Faculty and Staff Computing Behaviours That Protector Expose Them or Others to IS Attacks. Doctoral Dissertation, East Tennessee State University. Available online: http://proquest.umi.com/pqdlink?did=1597602021&fmt=2&vtype=PQD&vinst=PROD&RQT=309&vname=PQD&TS=1316378955&clientid=79356. Date Retrieved: September 18, 2011.

Olivier, M. S. (2004). Information Technology Research. A Practical Guide for Computer Science and Informatics (2nd ed.). Van Schaik Production.

OnlineHashCrack.com (2013). The Truth About Facebook Password Hacking. Available online: http://www.onlinehashcrack.com/how_to_crack_facebook_account_the_truth.php. Date Retrieved: March 5, 2013.

Owoade, H. and Jacob, O. (2013). Automated Phishing Worms. Fifth International Conference on Infotech and Security, Nigerian Computer Society (NCS), Lagos Airport Hotel, Ikeja, Lagos

Pahnila, S., Siponen, M., and Mahmood (2007). Employees' Behaviour towards IS Security Policy Compliance. Proceedings of the 40th Hawaii International Conference on System Sciences. IEEE, 156-166.

Parr B. (2011). Facebook Begins Testing Friend Filters in News Feed. Mashable Inc. Available online: http://mashable.com/2011/09/08/facebook-news-feed-changes/. Date Retrieved: June 22, 2013.

Pather, S. and Remenyi, D. (2004). Some of the Philosophical Issues Underpinning Research in Information Systems: From Positivism to Criticalism. Proceedings of the 2004 Annual Research Conference of the South African Institute of Computer Scientist and Information Technologist on IT Research in Developing Countries. Stellenbosch, South Africa, 75:141-146, SAICSIT.

Paternoster, R., and Pogarsky, G. (2009). Rational Choice, Agency and Thoughtfully Reflective Decision Making: The Short and Long-Term Consequences of Making Good Choices, Journal of Quantitative Criminology 25(2), 103-127.

PCWorld (2010). Google hit With Lawsuit Over Google Buzz. Available online At: http://www.pcworld.com/article/189712/google_hit_with_lawsuit_over_google_buzz.html. Date Retrieved: July 21, 2011.

Pendriveapps (2013). Portable Password Recovery Category. Pendriveapps.com. Available online: http://www.pendriveapps.com/software/password-recovery/. Date Retrieved: September 15, 2013.

Potalinski E (2012). Facebook Privacy Loophole Allows Profile Stalking. Zdnet. Available online: http://www.zdnet.com/blog/facebook/facebook-privacy-loophole-allows-profile-stalking/10762 Date Retrieved: September 24, 2012.

POPI (2009). Protection of Personal Information Bill, Ministry of Justice and Constitutional Development (MJCD), Republic Of South Africa. Available online: http://www.justice.gov.za/legislation/bills/B9-2009_ProtectionOfPersonalInformation.pdf. Date Retrieved: September 24, 2012.

Prairienet (2011). Facebook. Prairienet, Community Informative Initiative, Graduate School of Library and Information Science, University of Illinois. Available online: http://www.prairienet.org/op/stories/the-sharing-process/facebook/. Date Retrieved: July 8, 2013.

Preece, J., Rogers, Y., and Sharp, H. (2007). Interaction Design: Beyond-Human Computer Interaction. Chichester: John Wiley and sons Ltd.

PriceWaterHouseCoopers (2008). Safeguarding The New Currency Of Business; Findings From The 2008 Global State Of IS Study. Pricewaterhouse Coopers. Available online: http://www.pwc.com/ en_GX/gx/information-security-survey/pdf/safeguarding_the_new_currency.pdf. Date Retrieved: August 3, 2012.

PriceWaterHouseCoopers (2010). Protecting Your Business – Security Awareness: Turning Your People Into Your First Line Of Defence. Available online: http://www.pwc.co.uk/eng/publications /protecting_your_business_security_awareness.html. Date Retrieved: July 25, 2011.

Rainer, R. K., Synder, C. A., and Carr, H. H. (1991). Risk Analysis for Information Technology. Journal of Management Information Systems, 8(1): 129-147.

Rand, D (2007). Threats when using online SNs. CSIS Security Group (a Danish IT security company. Available online: http://www.csis.dk/dk/forside/LinkedIn.pdf. Date Retrieved: June 8, 2013.

ReutersSummits (2010). Facebook CEO Challenges the Social Norm Privacy. Available online: http://www.reuters.com/article/idus174222527820100112. Date Retrieved: June 5, 2011.

Rich, M. and Ginsburg, K.R. (1999). The Reason and Rhyme of Qualitative Research: Why, when, and how to use Qualitative Methods in the Study of Adolescent Health. Journal of Adolescent Health, 25:371-378.

Richter, M. (2013). Reminder: Finishing the Removal of an old Search Setting. Facebook Newsroom. Available online: https://newsroom.fb.com/News/735/Reminder-Finishing-the-Removal-of-an-Old-Search-Setting. Date Retrieved: November 18, 2013.

Riphagen, D. (2008). The Online Panopticon: Privacy Risks for Users of SN Sites. Systems Engineering, Policy Analysis and Management. Delft University of Technology. Available online: http://www.repository.tudelft.Nl/assets/uuid:b80a1e56-a2b3.../riphagen%20d.pdf. Date Retrieved: June 18, 2011.

Lemos, R. (2012). Five Strategic Security Metrics to Watch. Security Dark Reading. Available online: http://www.darkreading.com/monitoring/five-strategic-security-metrics-to-watch/232601457. Date Retrieved: November 12, 2013.

Padayachee, I. (2013). A Model Representing the Factors That Influence Virtual Learning System Usage in Higher Education. A PhD thesis submitted at the School of Computing, University of South Africa (UNISA).

Roode, D. (2009). Overview of Research Practice and Research Methodologies. Seminal Presentation at the 2009 CSIR Research and Innovation Core Skills (RICS) Programme.

Ross, M. (2014). Facebook Turns 10: the World Largest SN in Numbers. ABC News, available online: http://www.abc.net.au/news/2014-02-04/facebook-turns-10-the-social-network-in-numbers/5237128. Date Retrieved: November 12, 2014.

Rubin, H.J. and Rubin, I.S. (2005). Qualitative Interviewing: The Art of Hearing Data (2nd ed.). Thousand Oaks, CA, San Diego United States of America. Stage Publications, Inc.

Ryan, D. (2011). The Importance of Social Networking to Your Business. Seoconsult. Available online: http://www.seoconsult.com/seoblog/social-networking-and-search-engine-optimization/the-importance-of-social-networking-to-your-business.html Date Retrieved: January 12, 2013.

Samuel, J. and Samson, P. (2012). Unsecured Users' behaviour on the SNs; the outcome of Poor Password Combinations. Symposium on Usable Privacy and Security (SOUPS'12), Pittsburgh, PA, U.S.A.

SANS (2012). Security Awareness Survey. SANS, Securing the Human. Available online: http://www.securingthehuman.org/media/resources/business-justification/security-awareness-survey.pdf. Date Retrieved: May 27, 2013.

Scandura, A. and Williams, E. (2000). Research Methodology in Management: Current Practices, Trends and Implication for Future Research. Academy of Management Journal, 143 (6), 1248-1264.

Sekaran, U. and Bougie, R. (2010). Research Methods for Business: A Skill Building Approach (5th ed.). Chichester: John Wiley & Sons, pp 1-488.

Segall, N., Doolen, T. L. and Porter, J. D. (2005). A Usability Comparison of PDA-Based Quizzes and Paper-and-Pencil Quizzes. *Computers & Education*, 45, 417-432. Date Retrieved: August 5, 2013.

Shamim, S. (2011). Top 10 Most Visited Websites in the World. Expert Review now. Available online: http://www.expertreviewnow.com/2011/02/top-10-most-visited-websites-in-the-world/. Date Retrieved: July 25, 2011.

Singh, M and Patterh, M.S. (2007). Security Functional Components for Building a Secure Network Computing Environment. Information System Security, Vol. 16(6): 332-343. Available online: http://0-search.proquest.com.oasis.unisa.ac.za/docview/229583008/13BC99AE1555BAB50DE/1?accountid=14648. Date Retrieved: January 20, 2013.

Slater, D. (2012). Security Metrics: Critical Issues. Security Leadership. Available online: http://www.csoonline.com/article/455463/security-metrics-critical-issues. Date Retrieved: November 12, 2013.

Smith, E. (2012). The True Cost of Cyber-Security – Why Your Company Should Invest in it. Enlight Research. Available online: http://www.enlightresearch.com/ideas/2012/7/9/the-true-cost-of-cyber-security-why-your-company-should-inve.html. Date Retrieved: August 1, 2013.

Smith M. (2011). Facebook @ tagging Etiquette – A Guide for Personal and Business Use. Mari Smith... In the Media. Available online: http://www.marismith.com/wp-content/uploads/2011/01/Facebook-@-tag-example.jpg. Date Retrieved: January 7, 2013.

Smith, C. (2013). The Planet's 24 Largest Social Media Sites, and Where Their Next Wave of Growth Will Come From. Business Insider. Available online: http://www.businessinsider.com/a-global-social-media-census-2013-10. Date Retrieved: December 9, 2013.

Socialbakers (2014). Southwest Airlines (@southwestAir) Twitter Statistics. Available online: http://www.socialbakers.com/statistics/twitter/profiles/detail/7212562-southwestair. Date Retrieved: December 25, 2014.

SocialCompare (2013). Google+ Vs Facebook Vs Twitter. Beta SocialCompare, Collaborative Comparison Engine. Available online: http://socialcompare.com/en/comparison/ google- plus-vs-facebook-vs-twitter-comparison-table. Date retrieved January 7, 2013.

Soghoian, C. (2008). The Next Facebook Privacy Scandal. CNET. Available online: http://news.cnet.com/8301-13739_3-9854409-46.html. Date Retrieved: October 12, 2011.

Solove, D.J. (2006). A Taxonomy of Privacy. University of Pennsylvania Law Review, 154(3), 477-560. Available online: https://www.law.upenn.edu/journals/lawreview/articles/ volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf Date Retrieved: January 10, 2013.

Sommers, K. and Robinson, B. (2004). Security Awareness Training for Students at Virginia Commonwealth University. In the Proceedings of the SIGUCCS'04, Baltimore, Maryland, pp. 379-380.

Spice, B. (2007). Carnegie Mellon Researchers Fight Phishing Attacks With Phishing Tactics. Available Online: http://www.cmu.edu/news/archive/2007/october/oct2_phishing.shtml. Date Retrieved: April 21 2012.

Stanton, J. M., Stam, K. R., Guzman, I., and Caldera, C. (2003). Examining the Linkage Between Organisational Commitment and Information Security. Proceedings of the IEEE Systems, Man, and Cyber netics Conference. Washington, DC.

Stanton, J.M., Stam, K.R., Mastrangelo,. Jolton, J. (2005). Analysis of end User Security Behaviours. Computers and Security, Vol. 24, 2005, pp 124-133.

Stephanou, A.T. and Dagada, R. (2008). The Impact of Information Security Awareness Training on Information. Security Behaviour: the Case For Further Research. Proceedings of the Information Security for South Africa - ISSA 2008, Innovative Minds, pp. 311-330, School of Tourism and hospitality, University of Johannesburg,, South Africa,. Available online: http://if08030.files.wordpress.com/2011/06/issa2008proceedings.pdf. Date Retrieved: August 28 2012.

Stock and Barto (2013). Password Tools. David Stock and Bill Barto Consulting. Available online: http://thedatalist.com/pages/Password_Tools.htm. Date Retrieved: April 15, 2013.

Strahilevitz, L.J. (2005). A Social Network Theory of Privacy, Law and Economics Programme, Faculty of Law, University of Toronto.

Strater, K and Richter, H (2007). Examining privacy and disclosure in a Social Networking community (poster). Symposium on Usable Privacy and Security (SOUPS'07), Pittsburgh, PA, U.S.A.

Sullivan, M. (2007). Is Facebook The New Myspace?. PC World (San Francisco). Available online: http:// www.pcworld.com/article/id,134635-c,categories/article.html. Date Retrieved: April 30, 2008.

Taber M. (2011). Maximum Security: A Hacker's Guide to protecting Your Internet Site and Network. Macmillian Computer Publishing. Available online: http://newdata.box.sk/bx/hacker/ch10/ch10.htm. Date Retrieved: April 16, 2013.

Toledano, Y. (2005). Use online Survey to get the Feedback you Need: Tools and Best Practices for Conducting Web Surveys. Available online: http://www.techsoup.org/learningcenter/internet/ page5048.cfm. Date Retrieved July 8, 2013.

Treadwell, I. (2006). The Usability of Personal Digital Assistants (PDAs) for Assessment of Practical Performance. *Medical Education*, 40, 855-861. Date Retrieved: August 5, 2013.

Trendmicro (2012). The Human Factor in Data Protection. Ponemon Institute LLC. Available online: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-executive-summary.pdf. Date Retrieved: November 19, 2013.

UN (2003). A/RES/57/239: Creation of a Global Culture of Cybersecurity Fifty-Seventh Session of the United Nations (UN) General Assembly -Resolution adopted by the General Assembly, New York, United Nations, pp 1-3. Available online: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf. Date Retrieved: September 15, 2014.

UN (2004). A/RES/58/199: Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures. Fifty-Eighth Session of the United Nations (UN) General Assembly - Resolution adopted by the General Assembly, New York, United Nations, pp 1-3. Available online: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf. Date Retrieved: September 15, 2014.

UN (2010). A/RES/64/211: Creation of a Global Culture of Cybersecurity and taking stock of national efforts to protect Critical Information Infrastructures. Sixty-Fourth Session of the United Nations (UN) General Assembly -Resolution adopted by the General Assembly, New York, United Nations, pp 1-3. Available online: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/210. Date Retrieved: September 15, 2014.

Van Biljon, J. (2006). A Model for Representing the Motivational Cultural Factors That Influence Mobile Phone Usage Variety. Ph.D. Dissertation, School of Computing, University of South Africa (UNISA), South Africa.

Van Den Hoven, J. (2007). Information Technology, Privacy and the Protection of Personal Data. University Press, Cambridge, UK ; New York, Pp. 462-494. Available online: http://Lccn.Loc.Gov/2007016850. Date Retrieved: August 1, 2012.

Van Den Hoven, J. and Manders-Huits, N. (2006). Identiteits management En Morele Identificatie. Algemeen Nederlands Tijdschrift Voor Wijsbegeerte, 98(2):111-128.

Van Niekerk, J. and Von Solms, R. (2004). Organizational Learning Models for Information Security Education. A Proceeding of ISSA 2004, Johannesburg, South Africa.

Vaughan-Nichols, S.J. (2013). Facebook Remains top SN, Google+, YouTube Battle for Second. ZDNet. Available online: http://www.zdnet.com/facebook-remains-top-social-network-google-youtube-battle-for-second-7000015303/. Date Retrieved: July 9, 2013.

Veseli, I. (2011). Measuring the Effectiveness of IS Awareness Programme. Master Thesis, Master of Science in Information Security, Department of Computer Science and Media Technology, Gjovic University College. Available online: http://brage.bibsys.no/hig/bitstream/URN:NBN:No-bibsys_brage_21083/1/Ilirjana%20veseli.pdf. Date Retrieved: March 5, 2012.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2004). User Acceptance of Information Technology: Toward a unified view. MIS Quarterly, 27(3), 425–478.

Verenikina, I. (2001). Cultural-Historical Psychology and Activity Theory in Everyday Practice. In: Hasan, E. H G, P. Larkin & L. Vrazalic ed. 2001. Information Systems and Activity Theory: Volume 2 Theory and Practice. Wollongong: University of Wollongong Press. pp. 23-38.

Vroom, C. and Von Solms, R. (2004). Towards Information Security Behavioural Compliance. Computers and Security, 23(3):191-198.

Walzer, M. (1983). Spheres of Justice: A Defense of Pluralism and Equality, Basic Books. Available online: http://www.questia.com/library/4942736/spheres-of-justice-a-defense-of-pluralism-and-equality. Date Retrieved: September 19, 2011.

Wamala, F. (2012). The ITU National Cybersecurity guide, International Telecommunication Unit (ITU), Switzerland, Geneva. Available online: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf. Date Retrieved: August 25, 2014.

Weiss, S. (2007). Online SNs and the Need for new Privacy Research in Information and Communication Technology. Available online: http://www.cs.kau.se/IFIP-summerschool/summerschool2009/IFIP2007POST/papers/s04_p1_stefan_weiss.pdf. Date Retrieved: May 1, 2011.

Wikipedia, (2012a). Facebook. Wikipedia, the Free Encyclopedia. Available online: http://en.wikipedia.org/wiki/facebook. Date Retrieved: August 1, 2012.

Wikipedia (2012b). Social Networking Service. Wikipedia. Available online: http://en.wikipedia.org/wiki/social_network_service. Date Retrieved: September 23, 2012.

Williams, A. (2007). The Ineffectiveness of User Awareness Training. Available Online: http://techbuddha.wordpress.com/2007/05/02/the-ineffectiveness-of-user-awarenesstraining/. Date Retrieved: March 3, 2011.

Wilson, M. and Hash, J. (2003). Building an Information Technology Security Awareness and Training Programme. National Institute of Standards and Technology, NIST Special Publication 800-50, Technology Administration U.S.A. Department Of Commerce. Available Online: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf. Date Retrieved: June 7, 2012.

Wolf M.J. (2010). Measuring Information Security Awareness Programme. Master's Thesis, Department of Information Systems and Quantitative Analysis, University Of Nebraska, Omaha.

X-byaeger (2010). Best Practices – The Principle of Least Privilege (POLP). McAfee Communities. Available online: https://community.mcafee.com/docs/DOC-1455. Date Retrieved: June 18, 2013.

Yngström, L And Jörck, F. (2010). The Value and Assessment of IS Education and Training. Department of Computer and Systems Sciences, Stockholm University and Royal Institute of Technology, Electrum 230, SE-164 40 Kista, Sweden. Available Online: http://people.dsv.su.se/~bjorck/files/infosec-education.pdf. August 2, 2012.

LIST OF APPENDICES

Appendix A: Formal ethical clearance from UNISA

UNISA | college of science, engineering and technology

Julius Okesola (489448535)
School of Computing
UNISA
Pretoria

2013-06-09

Permission to conduct research project

Ref: 061/JOO/2013

The request for ethical approval for your PhD in Computer Science research project entitled "Measuring Information Security Awareness (ISA) Effectiveness In Social Networking Sites (SNS) – A Non-incident Statistic Approach" refers.

The College of Science, Engineering and Technology's (CSET) Research and Ethics Committee (CREC) has considered the relevant parts of the studies relating to the abovementioned research project and research methodology and is pleased to inform you that ethical clearance is granted for your study as set out in your proposal and application for ethical clearance.

Therefore, involved parties may also consider ethics approval as granted. However, the permission granted must not be misconstrued as constituting an instruction from the CSET Executive or the CSET CREC that sampled interviewees (if applicable) are compelled to take part in the research project. All interviewees retain their individual right to decide whether to participate or not.

We trust that the research will be undertaken in a manner that is respectful of the rights and integrity of those who volunteer to participate, as stipulated in the UNISA Research Ethics policy. The policy can be found at the following URL:
http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf

Please note that if you subsequently do a follow-up study that requires the use of a different research instrument, you will have to submit an addendum to this application, explaining the purpose of the follow-up study and attach the new instrument along with a comprehensive information document and consent form.

Yours sincerely

Chair: School of Computing Ethics Sub-Committee

University of South Africa
College of Science, Engineering and Technology
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone + 27 12 429 6122 Facsimile + 27 12 429 6848
www.unisa.ac.za/cset

Appendix B: Invitation letter to attend awareness presentation

October 30, 2011.

Dear Sir/Madam,

INVITATION TO ATTEND INFORMATION SECURITY AWARENESS PRESENTATION

I am a Doctoral student at the School of Computing, University of South Africa (UNISA). I am researching on the measurement of ISA efforts in SN. As part of my study, I have developed a social network (SN) – sOcialistOnline - for users to sign on and use at no cost. The essence of this SN is to gather research data sufficient enough for this study. To achieve this, there is a need for intended individuals with high esteem to sign on freely and use the network normally.

This presentation will offer me the opportunity to introduce some unique features of sOcialistOnline, and will also be a good medium to emphasis to the SN users the need for secured behaviours on SNs. The overall aim is to create awareness for my newly developed SN and attract more potential users.

You are therefore invited to a short presentation session organised as follows:

Date: November 7 and 8, 2011

Venue: TASUED Centre Auditorium, Ijebu-Ode, Nigeria

Time: 11am – 12noon

While your contribution is of utmost importance, I will like to mention that your attendance and participation is free, optional and may be anonymous. However, be assured that whatever information you provide is strictly for research purposes and will be treated with absolute confidence.

Thank you.

Julius OKESOLA.

48948535@mylife.unisa.ac.za

Appendix C: Example of informed consent for each UAT team member

October 16, 2011.

Dear Sir/Madam,

USER ACCEPTANCE TESTING – CONSENT FORM

I am a Doctoral student at the School of Computing, University of South Africa (UNISA). I am researching on the measurement of ISA efforts in SNs. As part of my study, I have developed a social network (SN) –sOcialistOnline - for users to sign on and use at no cost. The essence of this SNis to gather research data sufficient enough for this study. However, it is required to pass the system through a Users' Acceptance Test (UAT) before been moved to production for general use.

I therefore request for your expertise and time to participate in the UAT of sOcialistOnline using the attached testing scripts. You are however free to add to the scripts but please be guided by the scope of this study. Kindly document your exceptions for post - UAT discussions as soon as you are done.

While your contribution is of utmost importance, I will like to mention that your attendance and participation is free, optional and may be anonymous. However, be assured that whatever information you provide is strictly for research purposes and will be treated with absolute confidence.

Thank you for your time, patience and interest.

Julius OKESOLA.
48948535@mylife.unisa.ac.za

I, ----------

Hereby voluntarily agree to participate in the UAT exercise of sOcialistOnline.

Signature ---------- Date: ----------

Appendix D: The questionnaire transposed to quiz template

University of South Africa
School of Computing

QUESTIONNAIRE ON
INFORMATION SECURITY AWARENESS ON SOCIAL NETWORK

Dear Prospective Respondent,

I am a doctoral candidate in the PhD programme at the School of Computing, University of South Africa. I am carrying out a survey with the purpose of assessing the effectiveness of Information Security Awareness (ISA) efforts on SNs Sites. Please be assured that the information you provide is strictly for research purposes and will be treated with absolute confidence.

Press any key to Continue or N to Quit

INFORMED CONSENT

Please be fully informed as follows:

Right to Participate: Your response is of utmost importance to this exercise but you still reserve the right to participate. Your participation is voluntary and you are not under any obligation to oblige.

Right to Withdraw: We will appreciate your response to all the questions in the questionnaire. However, you have the right to determine the number and type of questions you are comfortable with, and you can withdraw from the questionnaire at any stage of this exercise without notice.

Right to Give Informed Consent: By continuing this questionnaire and submitting your responses to the questions, you give consent that your responses may be used in the study.

Right to Anonymity: You are not required to disclose your personal identity in this exercise. You may remain anonymous and still attend to the questionnaire adequately. In the event that your personal identity is disclosed, you can assured that the information you provide is strictly for research purposes and will be treated with absolute confidence and anonymity.

Right to Confidentiality: The essence of this exercise is to assess the effectiveness of Information Security Awareness (ISA) efforts on SNs Sites. Please be assured that the information you provide will be used strictly for the same purposes, and will be treated with absolute confidence and confidentiality.

Press any key to Continue or N to Quit

S/N	Questions	Answer/Options
	Knowledge	
1	Which of these is NOT a good way to secure your password from disclosure?	1. You may cram it 2. You may write it down anywhere visible and easily accessible 3. You may write it down but only in a secured place and with no title information 4. All of the above
2	When formulating a secure password, which of these could be used?	a. Names of family members, pets, and sports by appending a number at the beginning or end b. Misspelled words or phrases with numbers and special characters embedded c. Sequenced numbers and letters d. All of the above
3.	What will you do when somebody close to you (such as your brother) requests your Social Network's password?	a. Give it to him since he is a close associate b. Say No c. Ask questions, and give it to him if you are convinced d. All of the above
4.	Which one is not a good example of a strong password?	a. Simple and direct name of a close person (e.g. John) b. Meaningless combination that can easily be remembered (e.g. play2win+) c. Unrelated words combined together (e.g. sugar&meat) d. Misspelled words (e.g. Carpenter = Kafinta)
5.	In which of these ways can you be vulnerable to virus attacks on the Social Network?	a. Current virus protection tool is always enabled on your laptop b. System is always scanned anytime an image or a file is copied c. Unsolicited attachments are not opened d. Uploading of images to your Social Network wall from flash disks
	Attitudes	
6.	Which of these is in line with your belief about Information Systems safety and privacy on Social Network?	a. It is necessary and important b. It should be optional depending on what you have to protect c. It is entirely outside the user's control d. I am not concerned about privacy
7.	Which of the following security types do you believe represents the most important reasons behind online privacy on Social Networks?	a. Economic: Prevention of identity theft and protection of browsing habits from third parties b. Reputation: Protection of my social reputation by hiding my data and information c. Physical: Hiding my face and contacts from unknowns d. None of the above

S/N	Questions	Answer/Options
		Knowledge
8.	Are you worried about Social Network's privacy with respect to economic, reputation, or physical security?	a. I am not worried b. I am a little worried c. I am worried d. I am seriously worried
9.	Do you think settings on sOcialistOnline represent your attitude related to privacy?	a. Yes b. No c. sOcialistOnline does not have an appreciable privacy setting d. Privacy on Social Networks generally is all about management control
10.	Which of these describe reasons behind hiding your profile data such as hometown and gender?	a. The data may be potentially used for identity theft b. I don't feel safe and secured on Social Networks generally c. I just choose not to avail original details on my profile d. I don't hide any information
		Behaviour
11.	Which of these actions can help to safeguard your information on the Social Network?	a. Install a spam filter, current antispyware and antivirus software b. Leave my Social Network logon active even when I am not at the computer c. Both of the above d. None of the above
12.	Do you attend to security alerts that come up at logon about the strength of your password?	a. Yes b. No c. Not always d. One of the above
13.	Did you read and understand the policy document before signing onto sOcialistOnline?	a. Yes b. Yes, but only because it is easily comprehensible c. No, I don't have time for that d. No, because I am already used to the general Social Network's policy
14.	How often do you check your privacy controls and settings?	a. I check frequently b. I don't check c. I never checked again since setup d. Only when I am aware of a change on the site
15.	How cautious are you when meeting new friends online?	a. I accept friend requests from only those I am sure of. b. I accept only friends whose photos and information I admire c. I only accept friends from a certain niche d. All of the above

S/N	Questions	Answer/Options
Needs, objectives and experience or [normative and perceptions]		
16.	Why do you use Social Networks?	a. Connection to the social world b. Business entities (banking, airline, etc.) c. Academic d. All of the above
17.	Identify your social target behind using Social Networks	a. Meet new people and find old friends b. Join interest group (e.g. watch new movie free) c. Create albums for and share photographs d. I don't have any social target
18	What volume of personal data do you normally place on your Social Network profile?	a. My name and only one profile picture b. All information about me, including my addresses and family pictures c. My personal profile plus my business information and employment history d. Only my name and contact; not even my picture
19.	How can you describe your visit to Social Networks?	a. A regular user; always online 24 hours a day b. Occasional, at a specific interval (daily, weekly, monthly) c. Only when the need arises d. I cannot say
20.	What information leakage have you ever experienced on any Social Network?	a. None; I never had any b. Identity theft as my online account was hacked c. I was stalked by an unknown person who had unauthorised access to my information d. My acquaintances viewed my reputational information against my will

Appendix E: Privacy policy

SOcialistOnline

1. Information we receive about you

We receive a number of different types of information about you including your personal information and other data you choose to share. Personal information is your registration information that is required when you sign up for the site. At the point of signing up on sOcialistOnline, you are required to provide your name, e-mail address, birthday, and gender. Your information also includes the information you choose to share on sOcialistOnline, such as when you post a status update, upload a photo, or comment on a friend's post. It also includes information you choose to share when you take an action, such as when you add a friend, like a Page or a website, tag a place in your post, find friends using our contact importers, or indicate you are in a relationship.

2. How we use the information we receive

Your information is used with services and features we render to you and other users on our network, including our website developers and vendors. In particular, your information could be used as follows:

- For research purposes;
- To provide you with location features and services, like telling you and your friends when something is going on nearby; and
- As part of our efforts to keep sOcialistOnline safe and secure;
- To measure or understand the effectiveness of advertisements you and others see.

3. Ownership of the data

While we acknowledge that the information of the user is considered as his property and not belonging to the SN upon whose server it is stored, we request your trust that we will not share your information with others without your express permission. Otherwise, your name and any other personal identifying data will be removed from the information.

4. Account deactivation

An account that is deactivated will remain inactive until it is reactivated again by the registered user. This implies that the profile of such account can no longer be viewed by any SN user.

sOcialistOnline embraces this functionality and does not delete any of your information because of the likelihood of you coming back in the future.

5. Account deletion

An account that is deleted will be permanently removed from sOcialistOnline. Although some information may still remain in the backup copies and logs for a while, these information will not be available after two weeks when the deletion process would have been completed on sOcialistOnline. You are therefore advised to delete your account only if you are certain you are not coming back.

6. Control each time you post

- As a user, you are required to be very careful when posting because information shared on sOcialistOnline can be re-shared or copied by anyone who have access to the network.
- A user who posts content (such as a photo, status update or check-in), can customise his audience, or specify his group of audience. Where he fails to make a selection, his data may be shared with the audience he last selected. He can also change his selection later on his account profile.

Someone that you tag and his friends can see your post regardless of the audience you selected. The same is true when you approve a tag someone else adds to your post.

7. Your public information

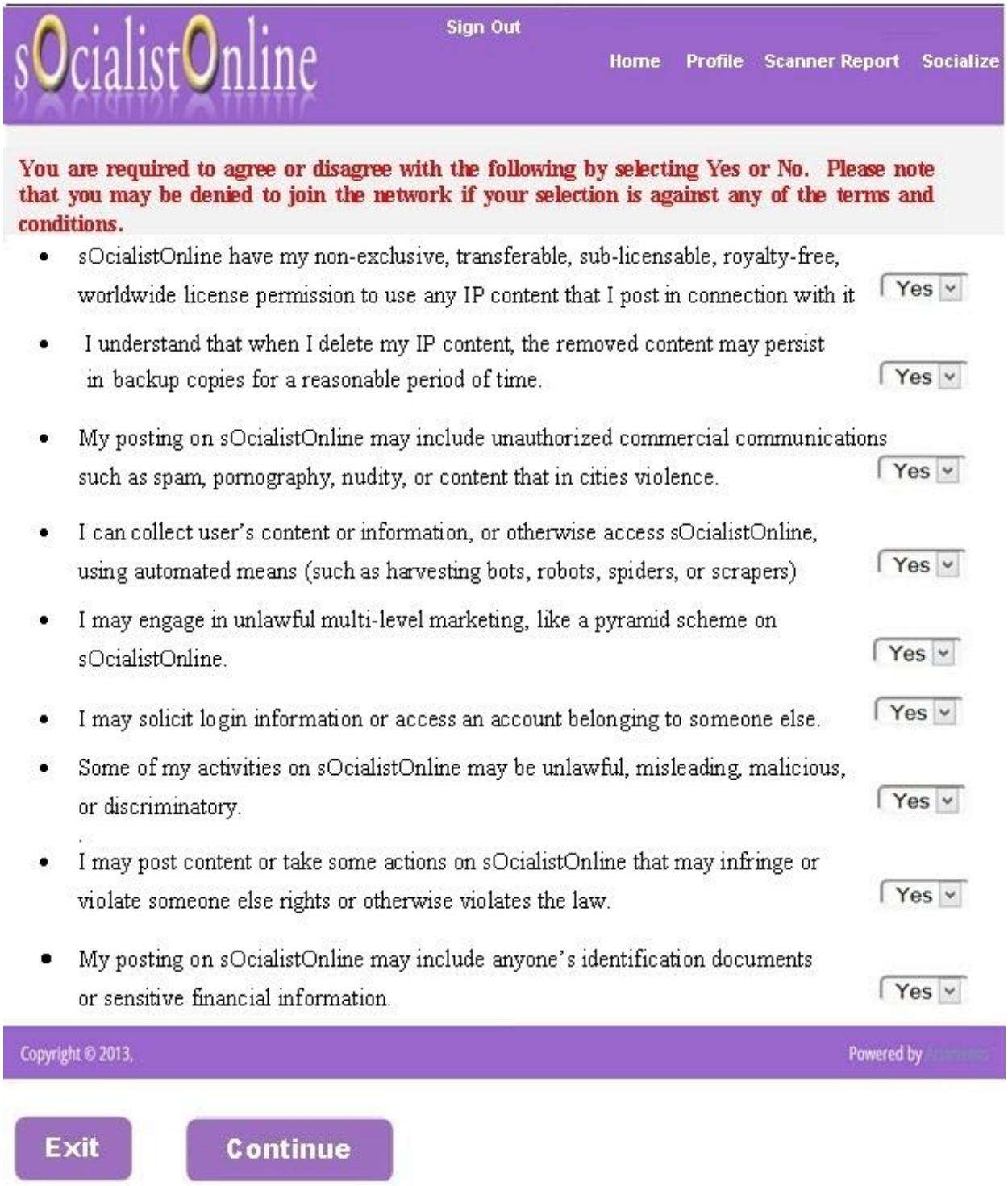
Generally, users' information such as name, user ID, profile pictures, username and network are treated public as they are often freely available to the general public. Users should therefore be fully aware that information being made public is easily accessible to everyone within and even outside sOcialistOnline. That is, such information can:

- Appear when there is a search on sOcialistOnline or on a public search engine;
- Be linked to the owner's name, picture, sOcialistOnline profile, User ID, etc.;
- Be used by the applications including games and websites that the user and his friends use.

8. Usernames and user IDs

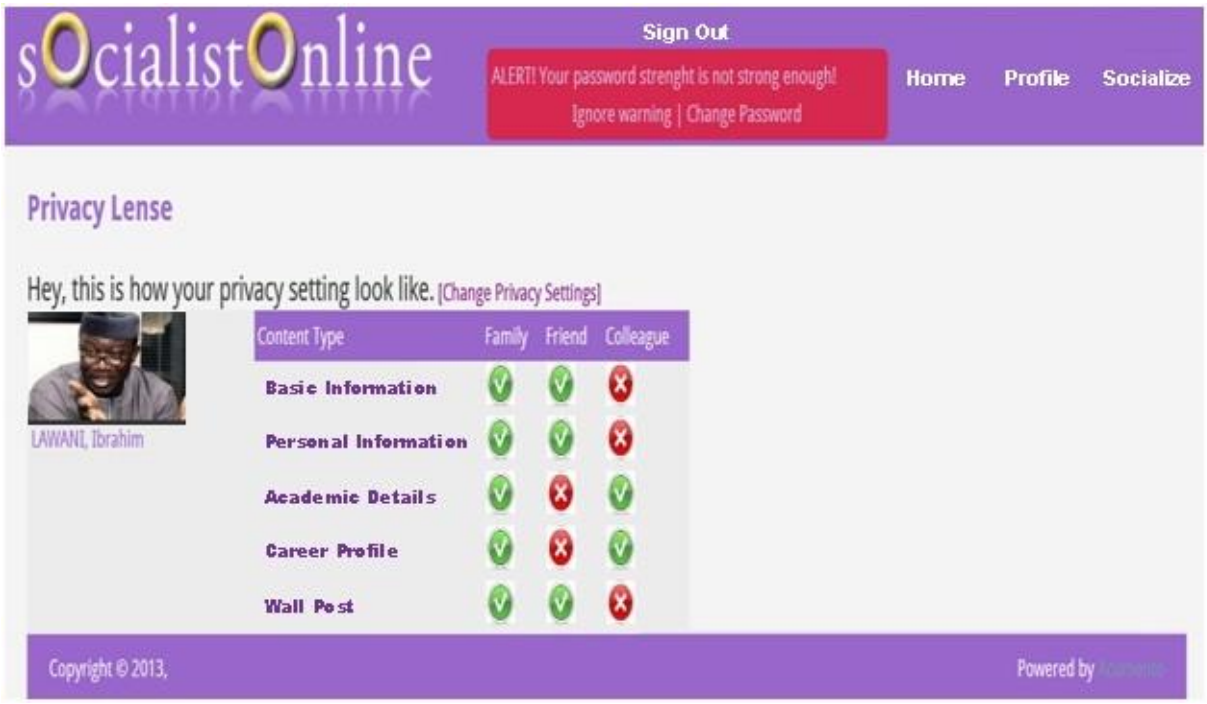
Someone with a user's valid username or user ID can access his/her information through sOcialistOnline website and Application Programming Interface (API). To prevent this, users are generally advised to turn off all platform applications from their privacy settings although, they may also not be able to access other applications.

Appendix F: User-friendly community guidelines



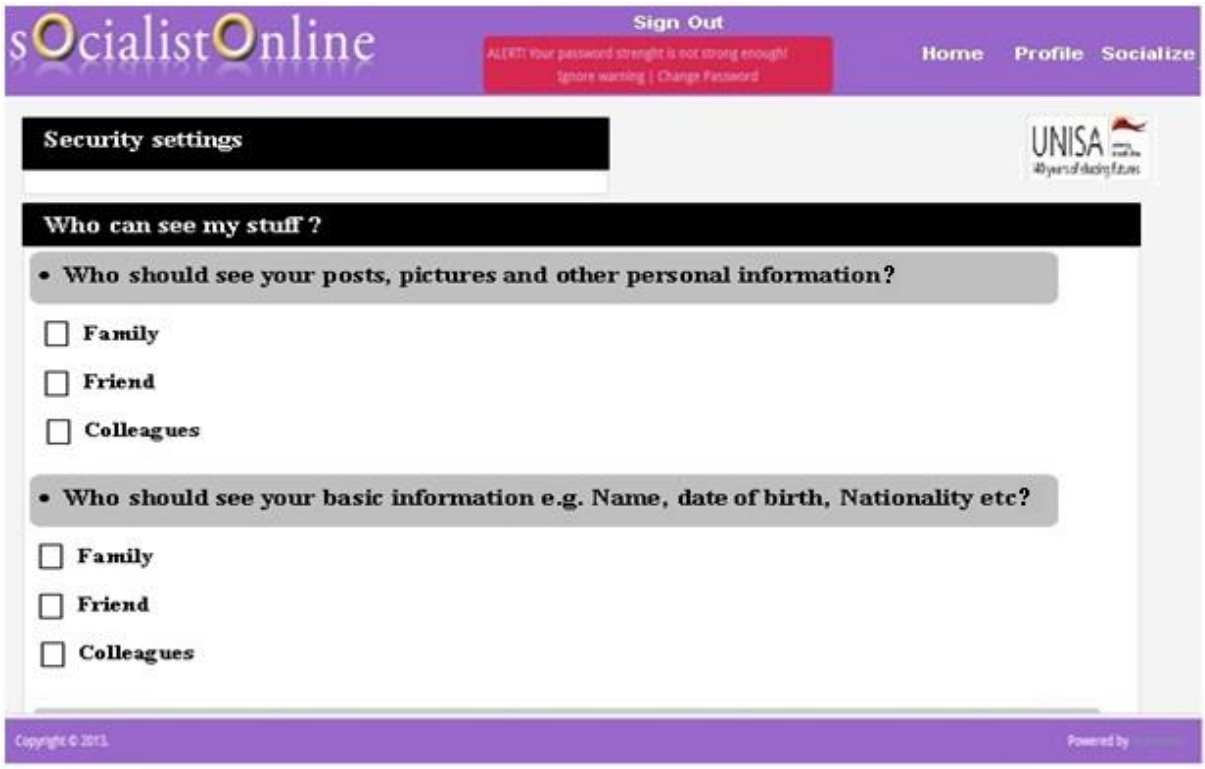
Appendix G: Screenshots of some awareness techniques

I. Privacy Lens



II. Password monitoring and standardisation (showing password alert)

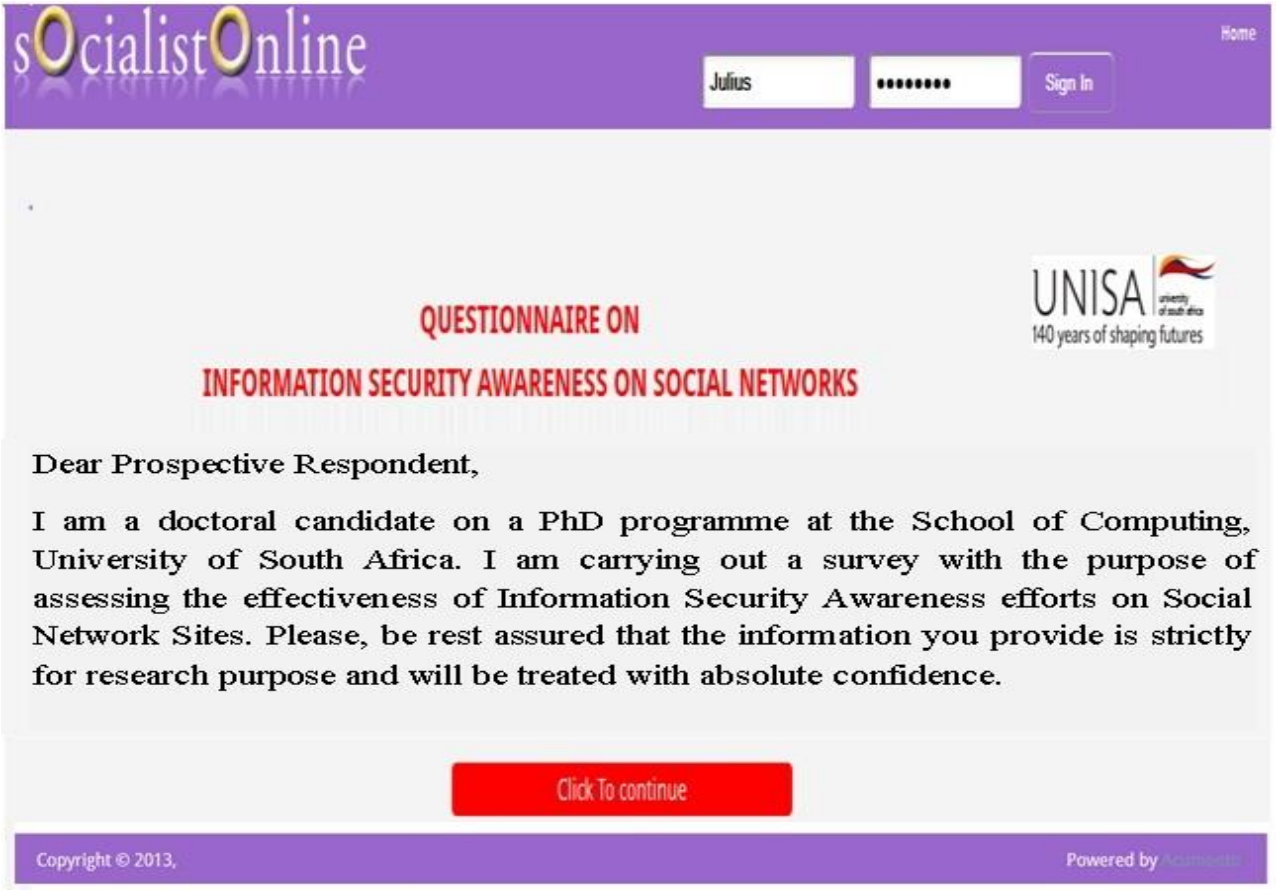
III. sOcialistOnline security settings



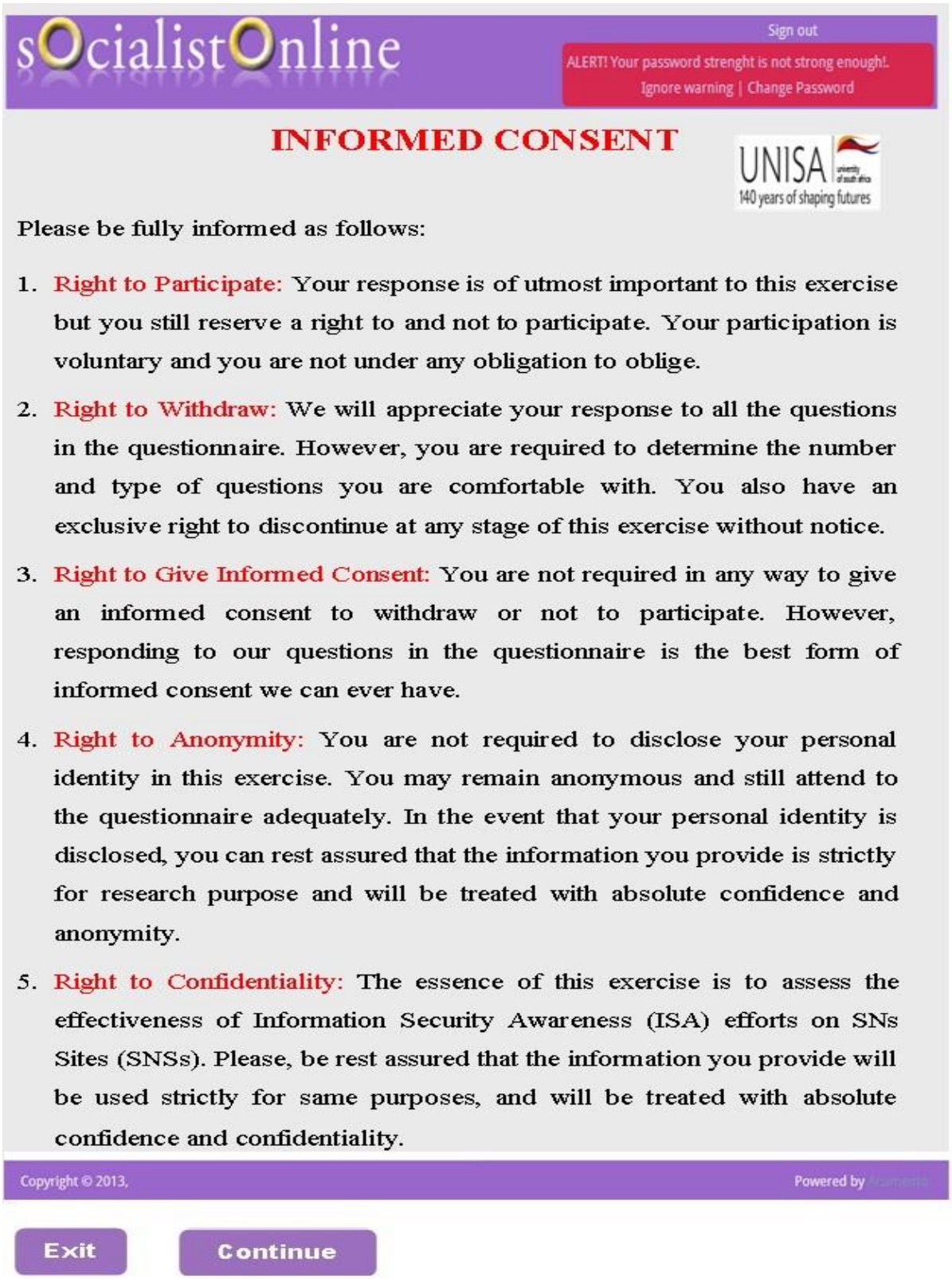
IV. Private messaging (showing password alert)

Appendix H: Screenshots from the quiz template

I. ***Screenshot of questionnaire***

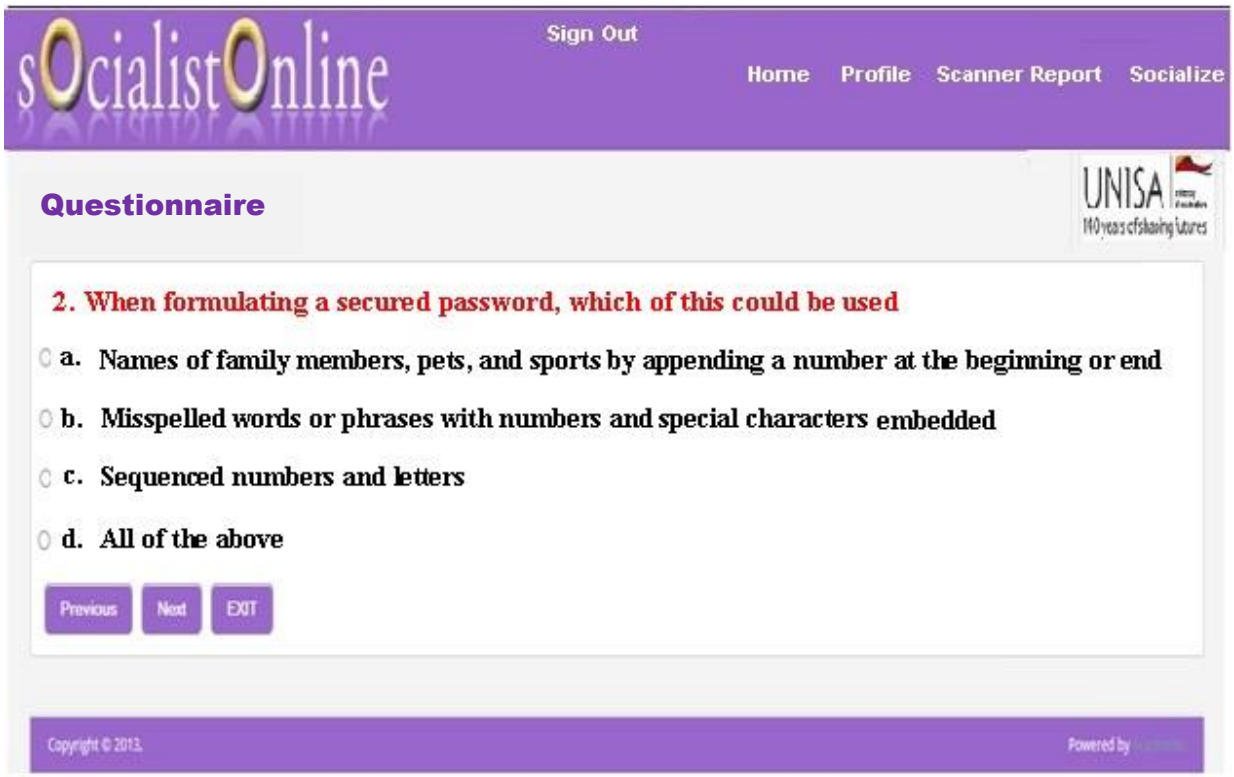


II. Informed consent accepted by the quiz audience

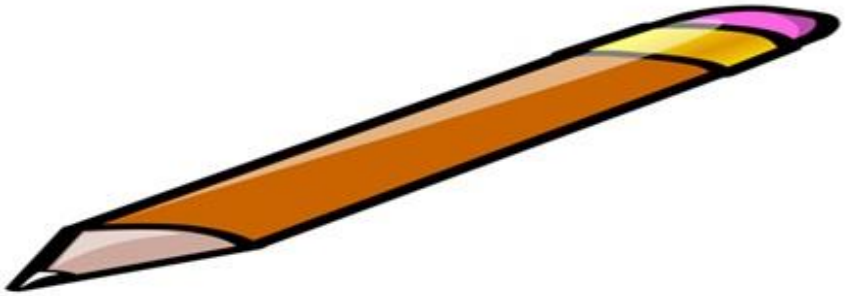


III. The first quiz

IV. The second quiz



Appendix I: Letter of certification from a qualified English language editor



Wena Coetzee trading as **WriteRight Solutions**

PO Box 164, Cresta 2118

Cell: 082 330 6304

18 January 2013

To whom it may concern

Letter of editing certification

This is to certify that the PhD thesis of Julius Olatunji **Okesola** has been edited and proofread by me, Dr Wena Coetzee, ID number 6305150012083, and that I have done everything in my power to make it as linguistically and technically correct as possible. I am a qualified language practitioner and translator and carry a doctorate in Applied Linguistics.

Yours faithfully

Dr Wena Coetzee

Appendix J: Acceptance letter from the testing team

July 12, 2014

Mr. Julius O. Okesola
School of computing,
University of South Africa (UNISA).

Dear Julius,

Validation Letter

The proposed social network is simple and the framework is straightforward. The practical controls implemented are okay and the various incorporated information security awareness techniques are adequate. The terms and condition is unique and social network will be inviting to many social network users.

If the social network is polished and publicized, it will be a preferred network globally as the users privacy is protected and social awareness is promoted.

Yours faithfully,

Dr. 

Director: 

Note:
Signature, name and directorate of the issuer of the validation letter were obscured for confidentiality

Appendix K: Validation report from ethical hacker

Aspa Security Solutions
IT Services and Supplies

1, Adeyemo Alakija Street
Victoria Island
Lagos
Phone: +234-8056-068-059
Email: info@aspa.com

June 24, 2014

To whom it may concern

Certification Letter

We are a group of professional ethical hackers employed to perform a penetrating test on sOcialistOnline and its password cracker for all the possible vulnerabilities against the hackers and other security threats.

We hereby certify that the social network and the password cracker are safe and adequately protected against all the possible internet and application threats.

Thank you.

Yours faithfully

Joshua O.AGUDA

Appendix L: A sample of the participant appraisal form

Evaluation of sOcialistOnline

Please take a few moments to complete this evaluation form. Your feedback is very important to continual program improvement.

Your Name (Optional)

Part One. Provide your reaction to the seminar by clicking on the radio button that matches your assessment. The rating scale is

1 = poor 2 = fair 3 = good 4 = very good 5 = excellent

		1	2	3	4	5
1.	What is your overall rating of this seminar?	○	○	○	○	◉
2.	What is your rating of the following aspects of the seminar?					
	a. Instructor's knowledge of the subject	○	○	○	○	◉
	b. Instructor's presentation style	○	○	○	○	◉
	c. Usefulness of print materials	○	○	○	◉	○
	d. Quality of the audio sounds	○	○	○	○	◉
	e. Extent the seminar met your expectations	○	○	○	○	◉

Part Two. Please describe your opinions about the seminar's strengths and weakness

3. What do you think were the weakness of the seminar?

THE DURATION WAS TOO SHORT

4. What do you think were the strength of the seminar?

THE SOCIAL NETWORK IS UNIQUE AND APPEARS PLAWLESS

5. How would you suggest this seminar be improved?

- STICK TO THE START TIME
- ALLOCATE ADEQUATE TIME FRAME

6. Any additional comments or suggestions?

NONE