# Guidelines to address the Human Factor in the South African National Research and Education Network Beneficiary Institutions

by

Yolanda Mjikeliso

2014

# Guidelines to address the Human Factor in the South African National Research and Education Network Beneficiary Institutions

by

**Yolanda Mjikeliso**

Submitted in fulfilment of the requirements for the degree

**MAGISTER TECHNOLOGIAE**

in

**INFORMATION TECHNOLOGY**

in the

**FACULTY OF ENGINEERING, THE BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY**

of the

**NELSON MANDELA METROPOLITAN UNIVERSITY**

Supervisor: **Prof. Johan van Niekerk**

Co-Supervisor: **Prof. Kerry-Lynn Thomson**

November 2014

# DECLARATION

Name: Yolanda Mjikeliso

Student Number: 209039445

Qualification: MTech IT

Research Title: Guidelines to address the Human Factor in the SANReN Network of Beneficiary Institutions

In accordance with Rule G4.6.3, I hereby declare that this treatise/dissertation/thesis is my own work and that it has not previously been submitted for assessment to another university or for another qualification.

Signature: ________________ Date: ________________

# ABSTRACT

Even if all the technical security solutions appropriate for an organisation’s network are implemented, for example, firewalls, antivirus programs and encryption, if the human factor is neglected then these technical security solutions will serve no purpose. The greatest challenge to network security is probably not the technological solutions that organisations invest in, but the human factor (non-technical solutions), which most organisations neglect. The human factor is often ignored even though humans are the most important resources of organisations and perform all the physical tasks, configure and manage equipment, enter data, manage people and operate the systems and networks.

The same people that manage and operate networks and systems have vulnerabilities. They are not perfect and there will always be an element of mistake-making or error. In other words, humans make mistakes that could result in security vulnerabilities, and the exploitation of these vulnerabilities could in turn result in network security breaches. Human vulnerabilities are driven by many factors including insufficient security education, training and awareness, a lack of security policies and procedures in the organisation, a limited attention span and negligence. Network security may thus be compromised by this human vulnerability.

In the context of this dissertation, both physical and technological controls should be implemented to ensure the security of the SANReN network. However, if the human factors are not adequately addressed, the network would become vulnerable to risks posed by the human factor which could threaten the security of the network. Accordingly, the primary research objective of this study is to formulate guidelines that address the information security related human factors in the rolling out and continued management of the SANReN network.  An analysis of existing policies and procedures governing the SANReN network was conducted and it was determined that there are currently no guidelines addressing the human factor in the SANReN beneficiary institutions. Therefore, the aim of this study is to provide the guidelines for addressing the human factor threats in the SANReN beneficiary institutions.

# ACKNOWLEDGEMENTS

To God be the glory for the things he alone has done!!
I would like to thank my Lord Jesus for giving me the strength and courage to embark on this journey.

This study would not have been possible without the help and support of the following people:

- My supervisor, Prof. Johan van Niekerk, you have moulded this study from the beginning to the end thank you for your constant guidance and support.

- My co-supervisor Prof. Kerry-Lynn Thomson, thank you for your endless support, guidance and motivation throughout this study.

- My parents, Samkelo Stofile and Luleka Mjikeliso and my loving family and friends who constantly reminded me that “Konke kuyenzeka xa ukholwa kuBawo”. Ndiyabulela!

- The financial assistance by the Vodacom/NMMU scholarship towards this research is also hereby acknowledged. Opinions expressed and conclusions arrived at are those of the author and are not necessarily to be attributed to the sponsors.

- The financial assistance of the National Research Foundation for this research is hereby acknowledged. The opinions expressed and the conclusions arrived at are those of the author and are not necessarily to be attributed to the National Research Foundation.

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# CHAPTER 1: INTRODUCTION

## 1.1 Background

Many years ago computers were mainly the territory of science, engineering and business (Kraut, Patterson, Lundmark, Mukopadhyay, & Scherlis, 1998). At that time, the Internet was used by a restricted community of computer experts and scientists only in order to share research and scientific information. However, in today's interconnected world the use of the Internet has become second nature to millions of people (Kritzinger & Von Solms, 2010). Today millions of people access the Internet which is no longer limited to a certain community of computer experts. According to Internet World Statistics, it is estimated that currently the Internet connects about 2.8 billion people all over the world and this population of people connected to the Internet continues to grow at a very fast pace (Internet World Stats, 2014).

The Internet is a network of hundreds of thousands of computers all over the world, which are connected in a way that allows other computers to access the information on them (Gray, 1999). For many Internet users Internet access has become an everyday activity that is used in schools, in universities, at work and in hospitals (Wellman, Quan-haase, Boase, & Chen, 2002). Many view the Internet as the life support that they use to sustain their lives. It is compared to water, food, air and shelter, and is seen as a constituent of life that is important for individuals to survive (Cisco, 2011). The Internet has changed the way people live, communicate and conduct business and has become a user-centric platform whereby users are able to access a significant amount of useful information (Kermarrec, 2013).

Owing to global Internet access people and organisations can share information instantly around the world (Jungck & Simon, 2004). Access to the Internet delivers a number of benefits; it enables the use of many services such as e-banking, e-health, e-learning and e-government (Furnell & Warren, 1999). However, while access to the Internet brings many advantages it also brings many disadvantages such as exposing computer systems to malicious actions that can cripple computers, businesses, government and people's lives (Jungck & Simon, 2004). Every day individuals, communities and nations are exposed to threats of cybercriminals – that is, people who conduct cybercrimes or display undesirable behaviour involving networked technology and the Internet (Hunton, 2011). The Internet may also expose vulnerabilities which can be exploited by people with the necessary technical skills (Furnell & Warren, 1999). Hackers, worms and viruses may cause disruption and damage to information systems and networks, with any computer that is connected to a network being under threat from virus and worm attacks by hackers (Hansman & Hunt, 2005). The threat of computer worms and viruses has grown into one of the greatest obstacles to the growth and reliability of the Internet and large networks (Jungck & Simon, 2004). The Internet is a vital part of national infrastructure and a key driver to socioeconomic growth and development (NATO, 2012). Moreover, the Internet connects many different National Research Networks (NRENs) from different countries around the world.

## 1.2 National Research and Education Network (NREN)

A National Research and Education Network (NREN) is a specialised Internet service provider for the research and education communities in a country. It provides research and education institutions (primarily universities) with services and access to the Internet. These services may also benefit other sectors, such as the healthcare sector. The management of NRENs from country to country differs, as the organisational and ownership model for each NREN varies. In some countries such as South Africa, the NREN is operated by the government, while in others it is run by a third party such as a university department under contract. A government institution, or the combination of a government institution and a third party such as a university department, can own an NREN (TERENA, 2009).

In South Africa there is a specialised Internet Service Provider (ISP) for the higher education and research sector known as the Tertiary Education and Research Network of South Africa (TENET) (UbuntuNet Alliance, n.d.). The TENET network provides Internet services to public universities, science councils and associated institutions; it does not provide such services to the commercial market. Therefore, all public universities and science councils in South Africa qualify to be part or a member of the TENET network (Martin, 2012). TENET provides Internet and related services to about 160 campuses of 54 institutions, including universities, research councils and other associated institutions (UbuntuNet Alliance, n.d.). The governing body of the SANReN network is the Council for Scientific and Industrial Research (CSIR) and the operational services of the SANReN network are provided by TENET to all beneficiary institutions on behalf of the CSIR (SANReN, 2014). A beneficiary institution (BI) is an institution that is defined by the Department of Science and Technology as one which is allowed to be connected to the SANReN network. These beneficiary institutions include the current TENET institutions such as universities and research councils (SANReN, 2014). The CSIR, which will be discussed in the following section, is the governing body of the SANReN network, while the entire NREN network infrastructure is operated by TENET.

## 1.3 South African Research Network (SANReN)

Governments around the world have embarked on a journey to bring fast, reliable and affordable Internet access to their citizens (NATO, 2012). One of the many networks interconnected to the Internet is SANReN, the South African National Research Network. SANReN is a high-speed communication network that is designed primarily for research institutions and organisations. This network, together with the Centre for High Performance Computing (CHCP) and Very Large Databases (VLDB), creates the key component of cyber infrastructure in South Africa (Meraka Institute, 2007). Accordingly, it forms part of the South African government's approach to cyber infrastructure; that is, to ensure the successful participation of South African researchers in global knowledge (Mooi, 2012b). The main purpose of SANReN is to provide South African research institutions and organisations with Internet access, as well as connecting them to research networks all over the world.

SANReN is a South African Department of Science and Technology (DST) project, implemented by the CSIR through the Meraka Institute. The SANReN project is being rolled out in a phased manner and will eventually connect up to 204 sites across South Africa, hosting over 3 000 education and research organisations from all over the world. The following section will discuss the network backbone of the SANReN network.

## 1.4 SANReN Network

The beneficiary institutions of the SANReN network are universities, research councils such as the CSIR, National Research Foundation (NRF) sites such as iThemba Labs, and various other research institutes (SANReN, 2014). The SANReN topology which is depicted in Figure 1–1 shows the backbone of the network. The SANReN network consists of a 10 Gpbs 7-

stretch backbone ring between the cities of Pretoria, Johannesburg, Bloemfontein, Cape Town, Port Elizabeth, East London and Durban, with a link from Durban to Pretoria to complete the redundant ring. These nodes, or SANReN Point of Presences (PoP), have been placed in all the connected institutions and the rollout of the SANReN is still progressing to other beneficiary institutions and organisations. The SANReN backbone will also reach remote towns, such as Butterworth, Kimberly and Nelspruit (Martin, 2012).

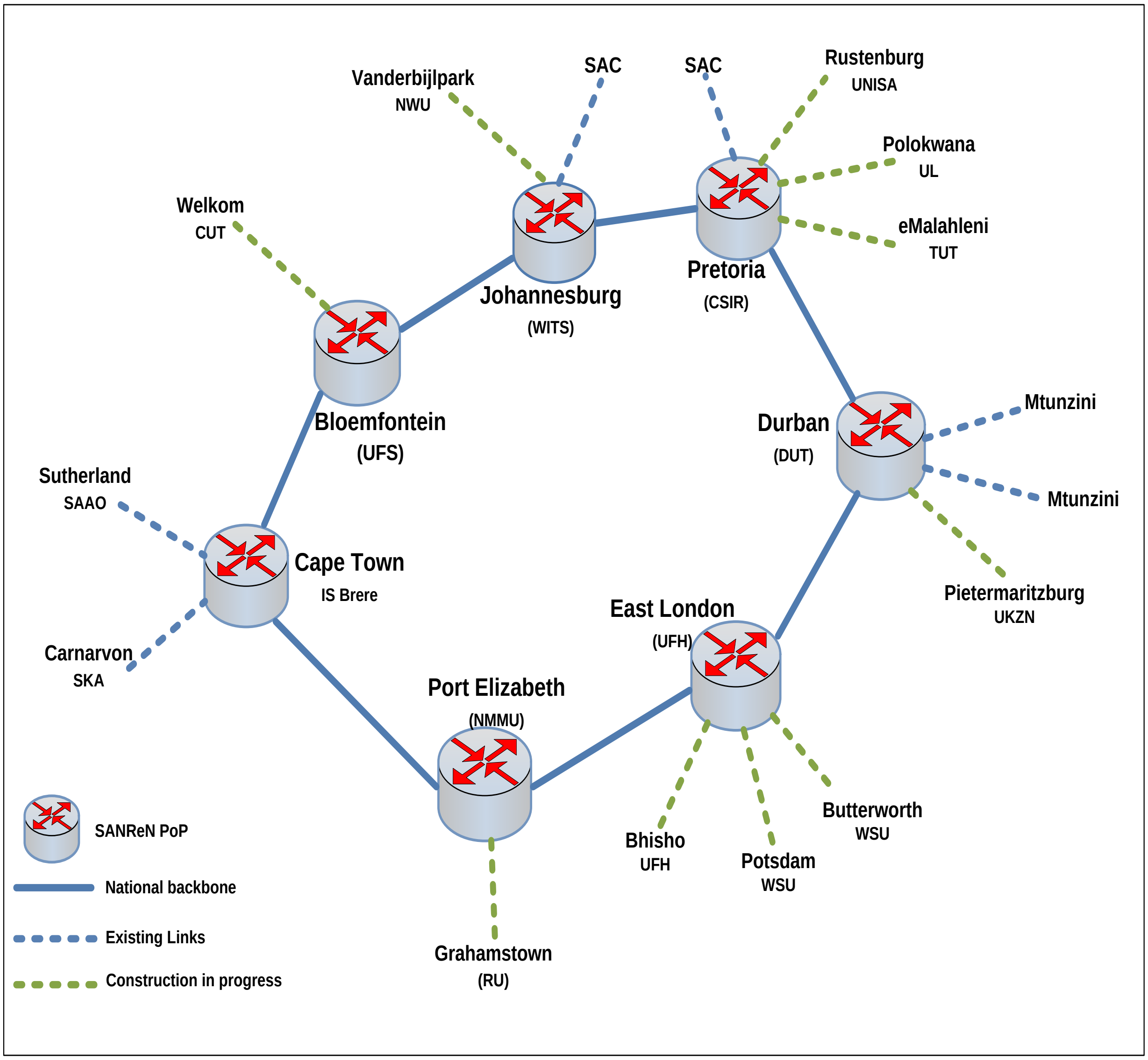

Figure 1-1: SANReN backbone (SANReN, 2013b).

SANReN has brought with it many opportunities and benefits to the people of South Africa. Rural areas such as Butterworth will have increased accessibility to the Internet, which could help in addressing the digital divide (SANReN, 2012). The digital divide, or the digital split, is a social issue that refers to the differing amount of information available to those who have access to the Internet and those who do not have access (Internet World Stats, 2012). The Internet, together with other information and communication technologies (ICTs), is in a way transforming society, eliminating power differentials and creating the realisation of a truly free and democratic world (Internet World Stats, 2012).

The SANReN network is one part of the cyber infrastructure attempting to close this digital gap. Consequently, the security of communication networks and systems is of increasing concern (Grobler & Bryk, 2010). As a result, many national and international security communities have started to work together in order to create a more secured Internet. This cooperation has led to the formation of the Computer Security Incident Response Team (CSIRT) (Grobler & Bryk, 2010).

## 1.5 Computer Security Incident Response Team (CSIRT)

A CSIRT is a group of people who are responsible for receiving and responding to network security incident reports and activities (Mooi, 2013). It is a group of dedicated information security specialists that are prepared for and able to respond to information security incidents (Grobler & Bryk, 2010). CSIRT teams provide the following benefits to the network of an organisation (Mooi, 2012a):

- Coordinate central response contact, thus building a shared knowledge of network incidents
- Provide specialised security expertise and incident-response resources
- Collaborate with other security teams as a trusted conduit
- Ensure compliance with policies and regulations

The SANReN team is in the process of establishing a SANReN/TENET CSIRT team, which will be responsible for managing security incidents in the SANReN network. The need for such a team was identified by a survey conducted in May 2012, which was sent out to all the beneficiary institutions of the SANReN network. The purpose of the survey was to investigate whether the beneficiary institutions would be interested in an incident response team, as there is no central point or central managing party available for handling incidents on the SANReN network. According to Mooi (2012a), the TENET Network Operations Centre (NOC) is responsible for handling network incidents. However, there may be restricted resources and the TENET team may lack effectiveness since they may be the only ones responsible for incident handling. The survey responses highlighted the need for a SANReN/TENET CSIRT team, because many beneficiary institutions indicated that they were experiencing difficulties with handling security incidents.

For example, one of the questions that were asked of the beneficiary institutions was: Do you have a security team?

- 70% of respondents from the beneficiary institutions indicated that their institution did have some form of IT security.
- 30% of the respondents indicated that they had no security team.

Another question that was asked was about formal training:

- Only 50% of respondents from beneficiary institutions indicated that the people on the team had had some kind of formal training for dealing with security incidents.
- 40% of respondents from the beneficiary institutions had had no formal training.
- 10% did not know whether their security team had received formal training.

Overall, about 80% of responses from beneficiary institutions highlighted the usefulness of an incident response team. The existence of the SANReN/TENET CSIRT will meet the needs of the beneficiary institutions and could possibly decrease the number of threats and incidents faced by them. This team will be responsible for protecting against all types of malicious activity on the SANReN network such as spam, denial of service attacks and hacking attempts. The team will be responsible for receiving, reviewing and responding to network security incidents (Mooi, 2012a). The role of the SANReN/TENET CSIRT is to protect the SANReN network, as well as the users or beneficiaries of the network (Mooi, 2012b). From a technical point of view, the SANReN network may be more secure because of this team. However, vulnerability may still be present in the security of the network in the form of what is known as the human factor, and this needs to be addressed.

## 1.6 Human Factor

“Don't rely on network safeguards and firewalls to protect your information. Look to your most vulnerable spot. You'll usually find that vulnerability lies in your people” (Mitnick, Simon, & Wozniak, 2002). This quote points out that the use of technical controls alone will not solve information security related problems. The overreliance on technology without considering other factors could have disastrous results. Accordingly, the management of information security depends on three elements, technology, processes and people. Nevertheless, although many organisations have become skilled at managing technology and processes they have been less successful at managing people (Ashenden, 2008). Many researchers agree that the human factor is one of the most significant vulnerabilities in information security and is often overlooked in organisations (Thomson & Von Solms, 2006; Kraemer & Carayon, 2007). Indeed, the use of technical controls alone will not ensure the safety of the information assets of an organisation and will not solve information security related problems. Consequently, people are said to be the greatest threat to information security, whether intentionally or through negligence or a lack of knowledge (Van Niekerk & Von Solms, 2010).

It is important for senior management in organisations to understand that information security is not a technical or physical issue; there are operational issues that depend on human behaviour (Thomson & Von Solms, 2006). Computers and the Internet are dependent on human beings for information and it should be borne in mind that the data available on the Internet was captured and created by human beings. The problem with humans is the fact that they have limited attention and accuracy – they make mistakes or errors (Ashton, 2009).

According to Swain and Guttman (1983) there are five different types of human factor errors that could result in information security breaches. The first one is called the ‘acts of omission’. This is a human factor error whereby people forget to perform a necessary action, for example, a failure to regularly change their passwords. The second human factor is the ‘acts of commission’. This is where people perform an incorrect procedure or action, such as writing down a password. The third human factor is the ‘extraneous acts’. These errors involve doing something that is unnecessary. The fourth human factor is the ‘sequential acts', which involves doing something in the wrong order or format. Finally, the fifth human factor is ‘time errors’. The main cause of human factor time errors is people who fail to perform a task within the required time, which could lead to security breaches (Swain & Guttman, 1983).

Related to these human factors, is the tendency for people to follow a certain routine without properly considering the consequences of that action. For example, clicking the ‘OK’ button without fully understanding the reason for that action. Furthermore, many security procedures depend on human memory and, by nature, the capacity of human memory is limited. The limited human memory is one of the factors that could result in the decrease of network security. For example, many anti-virus updates and other security patches require human intervention. However, due to the limitations associated with human memory, such procedures may not be carried out, which could lead to security breaches in the network (Parsons, Mccormac, Butavicius, & Ferguson, 2010). These types of human factor errors could exist in any organization that employs people, including the SANReN beneficiary institutions.

Many network attackers start their work by looking for vulnerabilities or weaknesses on the computer they can communicate with on the network targeted or even target an individual on the network. One possible threat to a network is if an attacker knows about a security flaw in the software that the network depends on and that the network administrator is unaware of (Ritchey & Ammann, 2000). Hence, because of human error most software packages will never be free of vulnerabilities (Grobler & Bryk, 2010). Another possible threat scenario would be if the network has hosts that are misconfigured because of a lack of the skills required to configure a secure system. Indeed, all networks have some level of vulnerability as it is impossible to eliminate such vulnerability completely (Ritchey & Ammann, 2000).

In each and every network, the human element plays a role. Humans are involved in configuring network devices, creating security policies or merely as end-users of the network. Consequently, all the people in an organisation need to understand their role and responsibility in network security in order to better protect the integrity, confidentiality and availability of information on the network. The people that the SANReN network connects and the people it employs may be its greatest vulnerability in its security. For example, employees working in an organisation (e.g. the SANReN or the beneficiary institutions) may use the authority granted to them gain access illegitimately to information systems within the organisation. This is referred to as an insider threat (Williams, 2008).

Insider threats can pose a security risk to the network because they involve legitimate access to the facilities, information and knowledge of the organisation and to the location of valuable assets. “The insider threat is like a tumor. If you realize there is a problem and address it, you will have short-term suffering but a good chance of recovery. If you ignore it, it will keep getting worse and while you might have short-term enjoyment, it will most likely kill you” (Cole & Ring, 2005). Cole and Ring (2005) thus compare the insider threat to a tumour, which if ignored will cause more and more harm to the security of the network. The main source of information security breaches is people and they remain the weakest link in the security chain. Because the human factor creates a hole on the security of the network, it is important that networks like SANReN properly address the vulnerability it causes. To this end, its end-users and IT staff must know their roles and responsibilities and adhere to correct procedures for protecting the network.

The rolling out of the SANReN network will indeed bring a number of opportunities and benefits to beneficiaries of the network. However, with these benefits come many potential risks because the SANReN network is connected to the Internet. This connectivity may expose the network to security threats and vulnerabilities. The next section will focus on the preliminary case study that was conducted to identify whether human factor vulnerabilities exist in the SANReN network.

## 1.7 Preliminary Case Study

A preliminary case study was conducted at Nelson Mandela Metropolitan University (NMMU), which is one of the universities participating in the SANReN network. The goal of the study was to determine the relationship between the SANReN network and the NMMU network, therefore an interview with the network administrator at NMMU was conducted. This was done in order to understand how the SANReN network is structured, how secure the network is and who manages the network at the different institutions that are connected to it.

When questioned about whether the management of the SANReN is distributed between all the universities that it connects, the network administrator mentioned that the SANReN is managed by TENET alone from its offices in Cape Town and Johannesburg. There are no people working for the SANReN network at the different universities connected to SANReN and the universities have no management or configuration access to the network devices. In terms of this arrangement, the universities host the network devices and the TENET team accesses the devices remotely or sends someone from SANReN (TENET) when configuration changes are needed on the network devices.

The network administrator was also questioned about the structure of the SANReN network, specifically as it relates to NMMU, and whether the NMMU and SANReN networks are isolated from one another, meaning could a failure on SANReN affect the NMMU network or vice versa. The network administrator mentioned that the SANReN and NMMU networks are isolated from each other and that although failure on the SANReN network could affect the connectivity to and from NMMU, it would not affect the actual NMMU network itself. As evidence of this, on 5 August 2013 there was a link failure on the SANReN backbone between East London and Durban and Bloemfontein and Cape Town. Consequently the NMMU network experienced slow Internet responses as a result of these link failures, but it was the only institution whose connectivity was affected.

When questioned about the security of the SANReN network, the network administrator was confident about both its technical and physical security: “We believe that the management of the SANReN is being done by some of the best IT professionals in South Africa, so in my opinion, I believe that the network configuration is as secure as necessary.” However, the network administrator also mentioned a human factor related incident where on one or two occasions the SANReN network administrators (TENET) managed to lock themselves out of the remote configuration session. They subsequently required local assistance from IT staff at NMMU to make the configuration changes required to the SANReN network device. Such a human factor related incident could potentially compromise the security of the network. This implies that although the network may be regarded as technically and physically secure, human factors may be the weakest link in the security of the SANReN network. After a perusal of the SANReN documentation it was found that none of the documents addresses the human factors involved in the SANReN network. Hence, there is no documented framework that deals with the security vulnerabilities posed by the human factor in the SANReN network.

## 1.8 Problem Statement

The SANReN network, which is being rolled out across South Africa, plays an important role in the Internet connectivity of South Africans. In order to ensure the continued availability of this connectivity this network needs to be secured. There are many physical and technological controls or technologies could be used to ensure the security of the network. Although from a technical point of view, network professionals who are knowledgeable regarding the SANReN network view this network as being adequately secured, the SANReN network's rollout strategy currently does not adequately address the human factor in information security. Since the human factor is generally the biggest threat to the security of a network, the SANReN network may be vulnerable to the risks it poses. Accordingly, the problem statement for this dissertation can be defined as:

The rolling out of the SANReN network has not formally considered the information security risks posed by the human factor on the networks of the beneficiary institutions.

## 1.9 Research Objectives

The problem that this research will address has been defined. This section will define the primary and secondary objectives of this research.

**Primary Objective**

The primary research objective of this dissertation will be to propose guidelines for addressing the information security related human factors in the rolling out and continued management of the SANReN network.

**Secondary Objectives**

In order to achieve the above primary objective the following secondary research objectives have been identified.

- *To analyse the current SANReN network in order to identify all the human factors that might increase security risks for the SANReN beneficiary institutions.*
- *To determine what literature recommends with regard to addressing the human factors in information security.*

- *To investigate the role of information security education, training and awareness when addressing human factors in information security.*
- *To verify with the aid of an appropriate methodology the applicability of the proposed guidelines*.

## 1.10 Methodology

The research methodology used in this dissertation is discussed in the following chapter (Chapter 2). This dissertation has been structured according to Creswell's structure of a case study.

## 1.11 Research Scope and Delineations

This research will focus exclusively on the human factors affecting the rolling out and management of the SANReN network as these human factors pertain to the SANReN beneficiary institutions.

## 1.12 Layout of the dissertation

The following diagram shows the chapter layout of this dissertation:

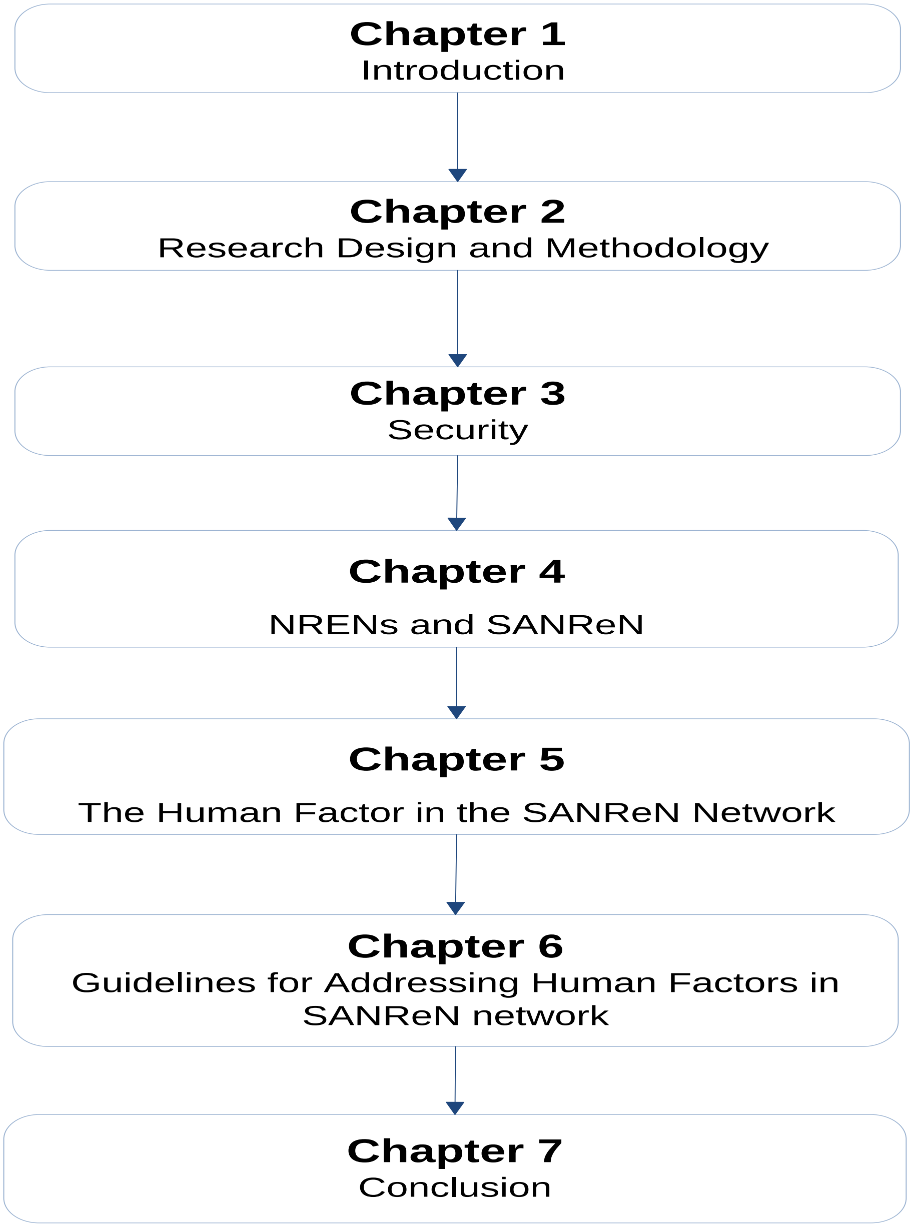
Chapter 1
Introduction
Chapter 2
Research Design and Methodology
Chapter 3
Security
Chapter 4
NRENs and SANReN
Chapter 5
The Human Factor in the SANReN Network
Chapter 6
Guidelines for Addressing Human Factors in SANReN network
Chapter 7
Conclusion

Figure 1-2: Layout of the dissertation

# CHAPTER 2: RESEARCH DESIGN AND METHODOLOGY

## 2.1 Introduction

*“Research design is a ‘blueprint’ for your research, dealing with at least four problems: what questions to study, what data are relevant, what data to collect, and how to analyze the results”* (Yin, 2014).

The main purpose of a research design is to avoid certain situations where the evidence does not address the initial research questions or initial objectives. This chapter will discuss the research design used in conducting this dissertation and it will also discuss the methods used to collect the data or the sources of evidence. The following section will discuss the research design that was followed in the study.

## 2.2 Research Design

Creswell (2009) makes a distinction between three different types of research design: qualitative, quantitative and mixed method. He argues that the difference between qualitative and quantitative research may be framed in terms of using words (qualitative research) rather than numbers (quantitative research), or using closed-ended questions (quantitative hypothesis) rather than open-ended questions (qualitative interview questions). The difference also becomes apparent in the type of research strategies used overall in the research, for example experiments in quantitative research and case studies in qualitative research (Creswell, 2009).

After the researcher has selected the research design to be used to conduct the study, a research strategy or methodology for achieving the required solution or outcome must be selected. Research strategies or strategies of inquiry are types of research design (quantitative, qualitative, mixed method) that provide specific direction for the procedures to be included in a research design (Creswell, 2009). Other researchers refer to strategies of inquiry as research methodologies or approaches to inquiry (Mertens, 1998).

This dissertation followed a case study approach (qualitative research design) as the overall methodology. Case study is a strategy of inquiry or research methodology in which the researcher explores in depth a programme, event, activity or process or one or more individuals. Case studies are bound by time and activity and entail researchers collecting detailed information using many forms of data collection procedures (Creswell, 2009).

Yin (2014) defines a case study as an empirical inquiry that investigates a contemporary phenomenon ("the case") in depth within its real-world context, especially when the boundaries between the phenomenon and its context may not be clearly defined. A case study methodology could be used when

- a "how" and "why" question is being asked about
    - a contemporary set of events
    - over which a researcher has little or no control

A case study approach was selected as the overall approach for conducting this study because it builds an in-depth contextual understanding of the issue (the case) being studied while relying on numerous data sources. Another reason why the case study method was selected is the need to address the human factor in the SANReN beneficiary institutions, meaning it is a real-life problem. In view of this, Yin (2014) maintains that the use of a case study allows the researcher to focus on a "case" and maintain a holistic and real-world perspective such as studying individual life cycles, small group behaviour, school performance and neighbourhood changes. Therefore the research problem that this study is trying to solve is a real-life problem. The following section will discuss the case study research method as described by Yin (2014).

## 2.3 Case study methodology

This dissertation made use of case study research, as recommended by Yin (2014). Yin suggests that six stages should occur when conducting a case study:

- Plan
- Design
- Prepare

- Collect
- Analyse
- Share

### 2.3.1 Plan

This is the initial stage of case study research. During this stage the researcher needs to show how a comprehensive methodical path will be followed. The researcher should begin this path with a thorough literature review and thoughtful research questions or objectives (Yin, 2014). Therefore, in this initial stage the objectives of the study were formulated (see Chapter 1) on the basis of the literature review and a content analysis. Accordingly, the primary objective of this dissertation is to "propose guidelines for addressing the information security related human factors in the rolling out and continued management of the SANReN network". In order to achieve this primary objective secondary research objectives were formulated (see section 1.9).

### 2.3.2 Design

The second stage in conducting a case study is defined by Yin (2014) as the logical sequence that connects the empirical data to the initial research objectives and, eventually, to the conclusion. According to Yin (2014), research design comprises a logical plan for moving from "here" to "there", where "here" could represent the research objectives to be achieved or the research questions to be answered and "there" could represent the outcome, conclusions or answers to the research objective or questions. Yin argues that between the "here" and "there" there could be a number of major steps such as the collection and analysis of relevant data (Yin, 2014). According to Creswell (2009), a research design is a plan or a proposal for conducting research; it includes the intersection of philosophy, strategies of inquiry and specific methods.

In this research a single case study was conducted, focusing specifically on NMMU. The case study was conducted by means of interviews with NMMU engineers and SANReN engineers. A survey was also planned for distribution to other beneficiary institutions; however, owing to the collaboration of SANReN engineers, this was deemed unnecessary because SANReN was not dealing with or addressing operational questions at the time and some of the data could be called "form" sources.

### 2.3.3 Prepare

The third stage in conducting case study research deals with all the preparations that have to be made before data collection begins. If the preparation process is not done well it can jeopardise the other stages of study. Yin (2014) argues that good preparation begins with the researcher having all the desired skills and values, such as the ability to ask good questions and interpret the answers fairly and the ability to be a good listener, as well as having a firm grasp of the issues being studied. Some of the tasks that the researcher must do during this stage include sharpening their skills as a case study researcher, conducting a pilot case study and gaining approval for the study in terms of the protection of human subjects. For the purposes of this dissertation, the researcher practised and developed all the required attributes and values. In addition, a preliminary case study was conducted to determine the existence of the research problem to be addressed, as well as to identify whether human factor vulnerabilities exist in the SANReN network.

### 2.3.4 Collect

This is the stage dealing with the collection of case study evidence. The data collection stage in case study research is an extensive phase and the data is drawn from multiple sources of information, such as observation, interviews, documents and audio-visual materials (Creswell, 2007). Yin recommends six sources of evidence: documents, archival records, interviews, direct observation, participant observations, and physical artefacts. This research study collected evidence using a literature review, semi-structured interviews and SANReN documentation. The semi-structures interviews were conducted with the network engineer at the beneficiary institution and with the network engineer from SANReN. The SANReN documentation, which included the SANReN/TENET policies, was also perused.

The literature review was also used to investigate the impact that information security education, training and awareness can have when it addresses human factors, as well as to identify what is recommended for addressing the human factors in information security. The data collected and the analysis of the data for the case study are discussed in Chapter 5.

### 2.3.5 Analyse

This stage involves the analysis of the case study evidence. During this stage the data collected in the previous step is analysed and interpreted (see Chapter 5). A qualitative content analysis (Krippendorff, 2004) was used to analyse and examine how and where on the SANReN network humans interact with or have access to the network. This content analysis was conducted on current SANReN documentation and SANReN policies to determine whether they address the human factors.

### 2.3.6 Share

This is the final stage in case study research where the conclusions, findings or results of the case study will be reported. These results or conclusions then have to be presented to an identified audience and it is consequently important that the researcher present relevant and sufficient evidence to ensure that the reader understands the study. A paper based on this research study was published and presented at the International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014) (see Appendix A). The HAISA conference was identified as the proper forum for sharing this research.

The above discussion presented the steps that should be followed when conducting case study research according to Yin (2014). The following section will discuss the research process followed in the study.

## 2.4 Research Process

The previous section discussed the stages of case study research following Yin's recommendations. This section will provide an outline or structure for case study research as given by Creswell (2009). Each of the chapters in this dissertation represents a component of the structure. Accordingly, this dissertation was structured in terms of the instructions and guidelines for qualitative case study research supplied by Creswell (2009) and Yin (2014). The entire dissertation will take the form of a case study and will follow the structure recommended by Creswell (2007) as follows:

- Entry vignette
- Introduction
- Description of the case and its context
- Development of issues
- Detail about selected issues

- Assertions
- Closing vignette

Chapter 1 of this dissertation serves as an *entry vignette* as well as the introduction to the case study. It provides the background to the research problem, the problem statement and the research objectives of the dissertation. An initial literature review was conducted to establish the human factors in information security and this was followed by a preliminary case study to further demonstrate the existence of the problem. The initial literature and the preliminary case study were followed by a more in-depth literature review in other chapters (Chapters 3 and 5) in order to establish how the human factors are currently being addressed in information security and whether the SANReN network currently addresses the human factor.

The *description of the case and the context* in which the case study occurs is provided in Chapters 1 and 4. Chapter 1 introduces the case, “addressing the human factor”, and its context, “the SANReN network”. This chapter (Chapter 1) provides a brief discussion of the human factors on the SANReN network. A more detailed description of the context of the case, that is, the SANReN network, is provided in Chapter 4.

The *development of issues* is discussed in Chapter 3, using a literature review to draw out the important and relevant security issues that the study must address. For example, matters discussed include the importance of information security, network security and related policies, security education training and awareness, and the human factors relating to networks. All these security aspects form or develop the foundational concept of the study.

Chapter 5 discusses the *detail about the selected issues.* The chapter examines in depth the human factor threats at beneficiary institutions. It also presents an analysis of the threats presented by the human factor that could threaten the security of the SANReN network.

The *assertions or lessons* learnt from the case study are presented in Chapter 6 (guidelines for addressing the human factor threats in SANReN beneficiary networks) and Chapter 7 forms the conclusion of the study, closing with the vignette.

## 2.5 Conclusion

This chapter discussed the case study methodology that was followed in this research. The overall structure or outline of the dissertation was presented according to Creswell's case study structure, and Yin's guidelines, or recommended stages for conducting a case study, were also employed. The next chapter will focus on a description of the context of the case – the SANReN network.

# CHAPTER 3: SECURITY

## 3.1 Introduction

*"Yesterday's security defenses are not effective against today's rapidly evolving threats"* (PricewaterhouseCoopers, 2010).

As technology advances, the technical security solutions that worked well in the past may not provide adequate protection today (Singh, 2009). Consequently, the challenge to the security of IT systems and networks might not be the technological solution that most organisations invest in, but rather the human factor (non-technical) which most organisations neglect (Ashenden, 2008; Furnell & Clarke, 2012; Ahmed, Sharif, Kabir, & Al-maimani, 2012). This chapter focuses on security. It begins with an introduction to security in general and then moves on to security domains, including information and network security. The chapter will also investigate the role people play in networks, as well as in information security, and will examine the factors that contribute to a secure network, such as policies, education, training and awareness.

## 3.2 Security Domains

Today, the Internet brings millions and millions of unsecured computer networks into communication with other networks. While these connections bring many benefits, they may also create security concerns. In this interconnected society, the security of each connected computer could depend on the security level of the other connected computers. In other words, the security of information stored in one computer could depend on the security level of other connected computers (Whitman & Mattord, 2012). Security may be defined as the quality or state of being secured from danger; it is a state of being free from harm (Whitman & Mattord, 2012).

According to the international standard, ISO/IEC 27032 (2012), security constitutes the protection of an asset from threats. A threat is a potential cause of an unwanted incident that may harm the protected asset (ISO/IEC 27032, 2012). Further, an asset is defined as something that is of great value to an organisation or individual which requires protection (NIST 800-16, 1998). An asset may require protection from natural disasters, power failures, theft or vandalism, network attackers, or undesirable events (Andress, 2011). For example, individuals who value their families and homes will do all they can to protect them and to ensure that they are safe. In order to do this they could install burglar bars and alarms and ensure that windows and doors are lockable (Ciampa, 2012). People may even have security cameras installed in their homes to ensure the protection of their families from criminals. In this case, the house and family are the valuable assets that require protection from threats (criminals).

As can be seen in Figure 3-1, the security environment includes various security domains such as cyber security, information security, network security, Internet security and ICT security, as well as Critical Information Infrastructure Protection (CIIP). As illustrated in Figure 3-1, cyber security is not identical to information security or any other security domain. It is in fact broader than information security, ICT security, network security and Internet security and requires stakeholders (organisations or people) to play an active role in it in order to maintain and improve the usefulness and trustworthiness of cyberspace (ISO/IEC 27032, 2012).

The following section will discuss these security domains by briefly elaborating on each. However, more emphasis will be placed on network security, as this is the main focus of this research. Information security will also be dealt with in more depth than the other security domains, since network security is the foundation of information security.

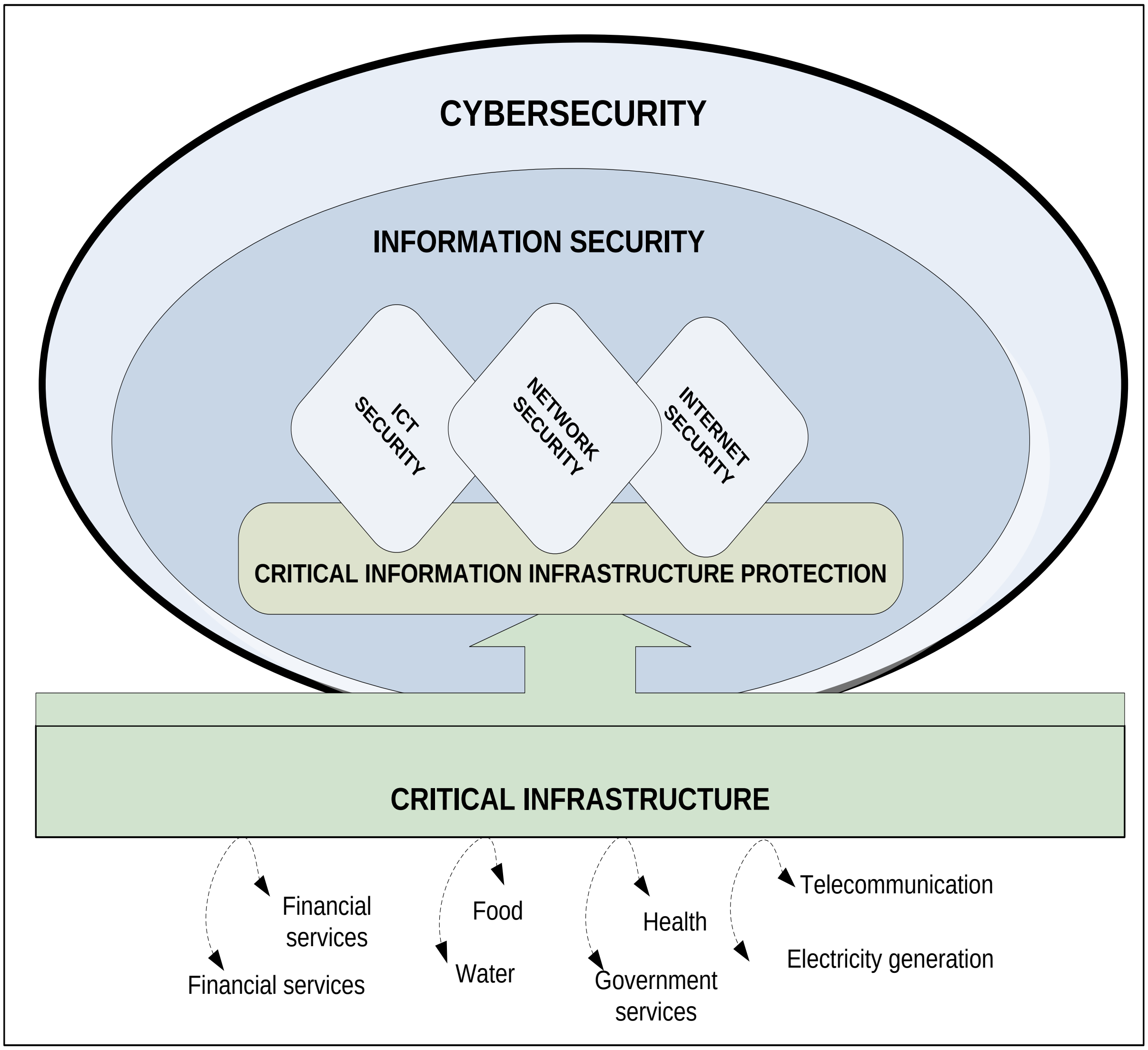

Figure 3-1: Relationships between security domains (ISO/IEC 27032, 2012)

## 3.3 Critical Information Infrastructure Protection (CIIP)

In many organisations one of the most valuable assets is information (Posthumus, Von Solms, & King, 2010). Information is the lifeblood of many organisations and in many organisations information technology (IT) systems are used to capture, store and process information. However, the biggest challenge posed by these systems is ensuring the security of an organisation’s electronic information, as they constantly expose information to many different threats (Von Solms & Von Solms, 2009). Since information is very often viewed as the glue that keeps organisations together, it is very important that it is secured; indeed, the success of the organisation could depend on it (Posthumus & Von Solms, 2004).

The systems and hardware that use, store and transmit information must be secure and, hence, the critical infrastructure (CI) that carries, uses, stores and transmits that information must be secured. CI consists of a nation's critical systems and assets, both physical or virtual, that require protection (NIST 800-16, 1998). Such infrastructure includes supply services (water, gas, energy, food, fuel), telecommunication (information and communication), electricity generation, transportation systems, financial services and other systems and services which are critical for the nation's welfare (Abou El Kalam, Deswarte, Baïna, & Kaâniche, 2009).

CI goes far beyond mere physical infrastructure to include data that is considered to be logical infrastructure or critical information infrastructure (CII) (Clemente, 2013). The term "CII" refers to interconnected computers, networks, the Internet, satellites, software and other critical information flows that are essential for the continuity of CI services (Cavelty, 2007). To a certain extent, CI relies on the CII in order to function properly (Hyslop, 2007). For that reason, the protection of the CII is of the utmost importance as it plays an important role in interlinking various infrastructure or CI sectors (health care, finance, energy etc) and is essential in ensuring that other structures are functioning properly at all times (Dunn & Wigert, 2004).

CI cannot be viewed independently from ICT, as ICT forms the supporting structure for CI by interconnecting and developing it globally (Theoharidou, Xidara, & Gritzalis, 2008). ICT is comprised of infrastructure that processes, stores and communicates information (Von Solms & van Niekerk, 2013). In other words, ICT can be described as the computing and telecommunications equipment, processes, software and people that support all the processing, storage and transmission of information (Dunn & Wigert, 2004). Most CI sectors rely on software-based control systems (information technology) and industrial control systems (ICS) to carry out their functions and this reliance on technology increases their vulnerabilities and the potential risk to operations (Cavelty, 2007). In Europe and the United States, for example, the majority of CII relies on computer communication systems for direct control and other functions (Goodman, 2008).

CI is becoming more complex and difficult to control because of its dependency on ICT. Consequently, this dependency of CI on ICT infrastructure may present some potential vulnerabilities (Theoharidou et al., 2008). It is therefore very important that this CI, as well as the CII that underpins it, is protected as the destruction, malfunction or failure of such structures would have a dramatic impact on the security, economy and social welfare of a nation (Kotzanikolaou, Theoharidou, & Gritzalis, 2013).

The term used describe the protection of CII is “critical information infrastructure protection” (CIIP). CIIP focuses on the protection of systems and networks provided or operated by CI providers, such as energy, telecommunication and water departments (NATO, 2012). CIIP is a subset of critical infrastructure protection (CIP), just as CII is a subset of CI. CIP is concerned with the protection of a country’s critical sectors or a nation’s infrastructure, while CIIP is concerned with the protection of the ICT sector and the CII underlying all other sectors (Dunn & Wigert, 2004). CIIP ensures that those systems and networks are protected against and made resilient as regards security risks relating to information, networks, the Internet, cyber space and ICT (ISO/IEC 27032, 2012), as these security domains all depend or rely on each other in some or other way. Figure 3-1 above illustrates the dependency or reliance between these security domains.

## 3.4 Cyber Security

In the context of the international standard, ISO/IEC 27032 (2012), the relationship between the various security domains and cyber security is very complex (ISO/IEC 27032, 2012). The term “cyber security” is often used interchangeably with the term “information security”; however, it can be argued that cyber security goes beyond the limitations of information security to include not just the protection of information resources but also the protection of other assets (Von Solms & Van Niekerk, 2013). Information security is the protection of the confidentiality, integrity and availability of information from the potential harm that could result from a variety of threats and vulnerabilities (ISO/IEC 27032, 2012). Cyber security or cyberspace security, on the other hand, relates to the preservation of the confidentiality, integrity and availability of information in cyberspace.

Additionally, the International Telecommunication Union (ITU), which is the United Nations agency for ICTs, defines cyber security as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, best practices, assurance and technologies that can be used to protect the cyber environment, as well as organisational and user assets. Organisational or user assets include all the connected computing devices, personnel, infrastructure, applications, services and telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment (Wamala, 2011).

Cyberspace can be described as a virtual environment that does not exist in any physical form. It is a complex environment resulting from the interaction of people, networks, software and services on the Internet. Cyberspace security or cyber security is about the security of this virtual world. However, because the existence of this virtual world depends on ICT devices and connected networks (ISO/IEC 27032, 2012), the security of these devices together with the connected networks is very important as these form the supporting structure for cyberspace. Accordingly, the availability and reliability of cyberspace relies on the availability and reliability of related CI services such as the telecommunications network infrastructure.

For example, water and transportation, which are CI services, have no major impact on cyber security. However, a lack of cyber security can have a negative impact on the availability of the CII systems (for water and transportation) provided by CI providers. It is therefore very important to understand that without network security, information security, Internet security and ICT security (security domains discussed in sections below) there would be no cyber security (ISO/IEC 27032, 2012). As depicted in Figure 3-1, cyber security is a broad security domain that to a certain extent encompasses all the security domains depicted in Figure 3-1. Hence, cyber security depends on information security, network security, Internet security and ICT security, as these are the fundamental building blocks of security (ISO/IEC 27032, 2012).

## 3.5 ICT Security

The security of ICT rests on certain information security principles; these include the confidentiality, integrity and availability of information existing on a particular computer system (NATO, 2012). In ICT security the asset to be secured is the underlying technology, while in the case of information security it is both the information and the underlying technology. In cyber security, on the other hand, any assets that can be accessed using cyberspace, that is, everything that functions in cyberspace, whether individuals or organisations, must be secured (Von Solms & Van Niekerk, 2013).

## 3.6 Internet Security

Organisations continue to flock to the Internet in increasing numbers, despite the fact that the overall Internet environment of the is not secure (Krause & Tipton, 2004). Accordingly, Internet security is concerned with protecting internet-related services, ICT systems and networks. Furthermore, Internet security is both an extension of network security and an element of information security (as shown if Figure 3-1) and thus, in order to achieve the purpose of security in organisations, it ensures the availability and reliability of Internet services in the organisation (NATO, 2012). The Internet, together with the ICT that supports it, are crucial national resources for governments and play a significant role in the socioeconomic growth and development of a nation or country (ISO/IEC 27032, 2012).

## 3.7 Information Security

Information is an asset just like any other business asset; it is of great value to the businesses and organisations (ISO/IEC 27002, 2007). An information asset refers to any tangible or intangible resource used to generate and use information; a business asset, on the other hand, refers to anything that provides value for an organisation, anything in which large investments in terms of money, time, worker skill and resources have been made. For example, a faulty desktop computer that could be easily replaced would not be considered an asset, unlike the information stored on that computer, which would be regarded as an asset to the organisation (Ciampa, 2012). Information is a valuable resource for many organisations since it supports all kinds of organisational decisions, therefore its protection is of the utmost importance (Kritzinger & Smith, 2008). Operational, tactical and strategic decisions are all supported by information (Raval & Fichadia, 2007). Such information may exist in many different forms; it can be printed on paper, stored electronically, transmitted electronically, shown on films, or communicated in conversations. Whatever the form information takes, it is important to ensure that it is always protected (ISO/IEC 27002, 2007).

Information security is the protection of the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission (Whitman & Mattord, 2012; ISO/IEC 27002, 2007). It is the protection of information from different threats in order to reduce business risk, ensure business continuity and increase return on investment and business opportunities (ISO/IEC 27002, 2007). Information security can be better understood by looking at its goal and how it is accomplished.

The goal of information security is to ensure that all the protective measures are properly implemented in order to protect the confidentiality, integrity and availability of information (Ciampa, 2012) and it is intended to provide protection for information that has value to people and organisations. However, it cannot guarantee the security of information; it can only create a defence system intended to prevent fatal system failure when an attack occurs. The same can be said with the security of a house; it can never be guaranteed even though proper security measures may be taken to secure the house. For example, you may install the best burglar bars, alarm systems and cameras, but this is not a guarantee that your house will be totally secure.

### 3.7.1 Importance of Information Security

Information security is important for both individuals and organisations (Ciampa, 2012). It is essential for protecting CI and the public and private sectors and may be essential in maintaining the competitive edge, cash flow, profitability, legal compliance and commercial image of the organisation (ISO/IEC 27002, 2007).

According to the International Organization for Standardization (2007), most information systems are not secure because security was not implemented during the design stage. The security obtained by technical means is limited and must accordingly be supported by management and procedures. It is important to note that information security management requires at the very least the participation of everyone in an organisation (including employees, shareholders, suppliers and third parties).

Ernst and Young (2008) conducted a global information security survey in which they asked the respondents to rate the impact or significance of an information asset. In other words, if an information asset is lost, unavailable or compromised what level of impact would that have on the success of the organisation, or if an information security incident were to take place how would it affect the organisation. According to the Ernst and Young survey, 85% of the survey respondents stated that the damage to the reputation and brand of an organisation is the most significant consequence of an information security incident. The other significant consequences include the following (Ernst & Young, 2008):

- Loss of stakeholder confidence (77%)
- Loss of revenues (72%)
- Loss of customers (71%)
- Regulatory action (68%)
- Legal action (65%)
- Damage to employee relationships (49%)

This shows that there are many consequences relating to the lack or compromise of information security. It clearly indicates why information security is an important business asset and why organisations should focus more in achieving information security (Ernst & Young, 2008).

The organisation’s reputation and revenue can take years to build, but all it takes is one information security incident to severely damage that reputation. Information security is a process; it is not a product or technology that can be purchased over a counter (Von Solms & Van Niekerk, 2013). The term “information security” can be defined in many different ways (as seen from section 3.7 above); however, most definitions concur on the preservation of the critical characteristics of information (confidentiality, integrity and availability). The following section will focus on these characteristics of information.

### 3.7.2 Critical Characteristics of Information Security

The key characteristics of information, which increase its value for an organisation, are confidentiality, integrity and availability, also known as the CIA triangle (Whitman & Mattord, 2010). Figure 3-2 below illustrates the relationship between these critical characteristics of information security. As discussed in the previous section (section 3.7), information security is about the preservation or protection of information and its critical characteristics; therefore it is important that information has these qualities in order for it to be secure.

The CIA concept can be compared to a three-legged stool. For a stool to be functional all the legs have to be the same length in order to achieve a sense of balance or stability. If one leg is shorter than the other legs, then the person sitting on the stool will fall off and the stool will have failed to serve its purpose. Similarly, if one of the critical characteristics of information security, namely, confidentiality, integrity or availability, is compromised, then the organisation's information will be of no use or of little value.

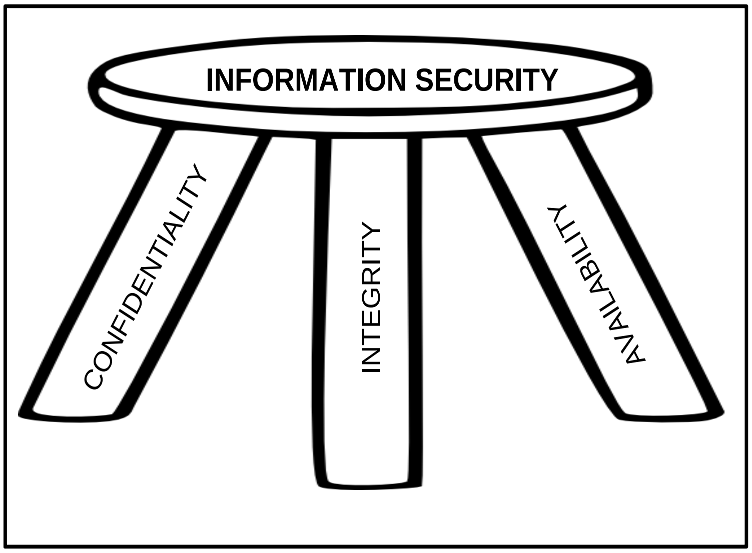

Figure 3-2: Critical characteristics of information (Hintzbergen, Hintzbergen, Smulders, & Baars, 2010; Whitman & Mattord, 2012).

#### 3.7.2.1 Confidentiality

The first leg of information security, confidentiality, refers to the ability to protect information from those who are not authorised to view it (Andress, 2011). It is concerned with ensuring that only those with sufficient privileges and a demonstrated need may have access to certain information. Confidentiality may be compromised or breached whenever an unauthorised individual or system gains access to or views certain information that they are not allowed to view (Whitman & Mattord, 2010).

For example, breach of confidentiality may occur when a person looks over your shoulder while you are typing in your password, an email attachment is sent to the wrong person, an attacker or hacker gains access to a bank database or credit card numbers are stolen from clients. The concept of confidentiality is closely related to privacy, but is not the same as privacy; in fact confidentiality is seen as one of the essential components of privacy (Andress, 2011). Confidentiality can be provided by limiting access to sensitive information only to authorised individuals, securing document storage, installing door locks to prevent access to networking devices, implementing general security policies, educating information custodians and end users, and encrypting sensitive information (Whitman & Mattord, 2010).

#### 3.7.2.2 Integrity

The second leg of information security, integrity, refers to the ability to prevent information from being changed in an unauthorised or undesirable manner (Andress, 2011). It is concerned with ensuring that information is correct and no unauthorised individual or malicious software has changed it. For example, if an attacker changes or alters patient information that contains the results of a medical test, the doctor might prescribe the wrong treatment which in turn might result in the patient’s death. This clearly demonstrates that integrity is very important especially when certain information will influence or provide the foundation for other decisions.

Integrity may be seen as the cornerstone of information security because information will have little or no value or use if its integrity cannot be verified. The integrity of information is compromised or threatened if it is exposed to corruption, damage, destruction or other disruption of its original form. Such corruption, damage or destruction of information may occur while information is being entered, stored or transmitted (Whitman & Mattord, 2010).

#### 3.7.2.3 Availability

The third leg, or characteristic, of information security is availability. Availability refers to the ability to access information by authorised users when they need it (Andress, 2011). Authorised users in this case may refer to a person or another computer system. Information that cannot be accessed when it is needed is essentially useless. Because information generally plays a critical role in organisations, they cannot afford to lose the accessibility of that information even for a short period. A lack or loss of availability may be the result of incidents such as virus attacks, power loss, application or operating system problems or human error (Raval & Fichadia, 2007).

The CIA triangle has been considered as the industry standard for computer security since the development of mainframes and these characteristics still as important today. Nevertheless, according to Whitman and Mattord (2010), ensuring the confidentiality, integrity and availability of information is not enough for information security because of the constantly changing environment of the computer industry. Other critical characteristics of information such as privacy, identification, authentication and accountability must also be considered because of the constantly evolving threats to information security today. Each of these additional critical characteristics of information will be discussed briefly in the following subsections.

#### 3.7.2.4 Privacy

Privacy is a characteristic of information when information is used, collected and stored. It ensures that information will be used only in ways that are known to the individual providing that information. Many organisations exploit people's privacy by collecting their personal information and subsequently exchanging it or selling it on to other organisations as a commodity. However, people are becoming aware of these poor practices and are expecting the government to do something to protect their privacy (Whitman & Mattord, 2010).

#### 3.7.2.5 Identification

Identification is the first step in obtaining access to secured material (information), and it serves as the foundation for subsequent authentication and authorisation. The difference between identification and authentication is that identification occurs when a user declares his or her identity to the system through the use of a user name or other ID (Whitman & Mattord, 2010).

#### 3.7.2.6 Authentication

Authentication is the process of ensuring that the individual is who he or she claims to be. It furthers the identification process by requiring proof of identity and it then verifies the validity of that identity (Ballad, Ballad, & Banks, 2010). In other words, it is the verification of what the user has claimed or declared to be his or her identity; this identity is verified through the use of a password, token or shared secret (Cole, 2009). Identification and authentication look at characteristics such as, Who you are? (biometrics), What do you have? (badge or identification document, token), What do you know?(password) (Raval & Fichadia, 2007)

#### 3.7.2.7 Accountability

Accountability takes place when the process of identification, authentication and authorisation has been successfully completed, or is in the process of being completed. It provides a way of tracing activities in any environment back to the source by tracing the identity of the person responsible for a certain activity and the privileges that have been given to that individual. This accountability process depends on the presence of identification, authentication and access control (Andress, 2011).

### 3.7.3 How to achieve Information Security in an Organisation

Information security may be achieved through the implementation of appropriate sets of controls, including policies, processes, procedures, organisational structures and software and hardware functions. These controls must be established, implemented, monitored, reviewed and improved in order to ensure that organisational objectives are met (ISO/IEC 27002, 2007). Controls such as policies must first be put into action by the organisation’s top management. Top management generally starts the policy cycle by aligning the organisation’s vision, rules and regulations with the policies. Ultimately, the main purpose of organisational policies is for management to dictate appropriate behaviour for employees (what is allowed and not allowed) (Von Solms & Von Solms, 2004).

The application of policies, education, training and awareness and technology are all necessary for achieving information security. Additionally, information security requires the organisation’s network operations to be secure. Network security is here concerned with the protection of the networks (systems and hardware) that use, store and transmit an organisation’s information (Whitman & Mattord, 2012).

## 3.8 Network Security

The lives of many people revolve around networks – we check our email, make phone calls, swipe to purchase goods using credit cards and access digital records (Lazer, Brewer, Christakis, Fowler, & King, 2009). Even the way people communicate has evolved tremendously over the years – in the past, people were restricted to face-to-face conversation. Today, thanks to advancements in communication technology, there are communication networks that can carry voice, text, graphics and video between different devices (Cisco, 2012). A computer network is a collection of connected computers – two or more computer systems are connected if they are able to send and receive data from each other through a shared-access medium. The access medium can refer to a physical cable connection between computer devices if the network is wired or fixed, or if the network is wireless then the access medium can involve some form of signalling, such as radio frequency (Douligeris & Serpanos, 2007).

### 3.8.1 Importance of Network Security

Computer networks have become assets to many organisations, which could not survive without their computer networks. Indeed, if disrupted they might find it impossible to conduct their business. Almost everything in organisations is done through computer networks; for example communication with suppliers, customers, employees and other organisations. Hence, the failure of network communication – thus limiting access to information on computers and a reliable communication system – could destroy the organisation (Cisco, 2012).

Networks need to be protected to prevent and reduce potential network attacks (Cisco, 2012). Thus, to secure data and mitigate threats, network protocols, technologies, devices, tools and techniques must be utilised. For this purpose, network security professionals are responsible for configuring firewalls and intrusion prevention systems, as well as ensuring data encryption in the organisation (Cisco, 2012).

In addition, these professionals are responsible for ensuring the integrity, availability and confidentiality of the information on the network. A secure network ensures the safety of both the organisational operations or functions and network users. In order for a network to be secure security professionals need to be vigilant with regard to new and evolving threats and attacks on the network that emanate from both outside and inside the network, whether the threats are intentional or accidental (Cisco, 2012).

### 3.8.2 Threats to Network Security

Almost every day new network and computer viruses appear that are difficult to track and prevent. Threats to network security are increasing in number and sophistication (Singh, 2009), with millions of security incidents in the form of viruses, hackers, spyware, spam, zombie networks and threats to information security (network security) (Huang, Rau, & Salvendy, 2010).

Table 3-1 below lists the most common threats to information security (network security). These threats differ from each other, and yet are similar in that they pose a risk to the availability, confidentiality and integrity of information. They also pose a danger to the organisation's systems, networks and employees (Whitman & Mattord, 2012).

| | **Category of threats** | **Examples** |
|---|---|---|
| **1.** | Human error or failure | Accidents, employee mistakes |
| **2.** | Software attacks | Viruses, worms, macros, denial of service |
| **3.** | Forces of nature | Fire, floods, earthquakes, lightning |
| **4.** | Missing, inadequate or incomplete | Loss of access to information systems resulting from disk drive failure without proper backup and recovery plan, no organisational policy or planning in place |
| **5.** | Missing, inadequate or incomplete controls | Network compromised because no firewall security controls |
| **6.** | Technical hardware failures or errors | Equipment failure |
| **7.** | Technical software failures or errors | Bugs, code problems, unknown loopholes |

| | | |
|---|---|---|
| **8.** | Theft | Illegal confiscation of equipment or information |
| **9.** | Espionage or trespass | Unauthorised access and/or data collection |

Figure 3-3: Common threats in information and network security (Whitman & Mattord, 2012)

There are two approaches that can be taken when implementing security: a reactive security approach and a proactive security approach. Most organisations demonstrate a reactive approach to security in terms of which they wait for a new virus, worm or incident to happen and then they react to the problem through system patching or reconfiguring the security of the system. Such an approach has little effect because, despite the response to the incident, the damage has already been done. A proactive security approach is considered to be the proper and most effective way of responding to security breaches. In terms of this approach, the vulnerabilities of critical assets are determined and controls put in place to address them (Cole, 2009).

For example, in December 2010, Sergey Aleynikov was found guilty of passing on trade secrets. At the time of the incident, he was working for a Wall Street company as a computer programmer. During his employment he transferred 32 megabytes of proprietary computer codes. Fortunately, the company discovered this abnormality through its routine network monitoring systems (FBI, n.d.). This theft could have cost the company he was working for millions of dollars, but because of the regular network monitoring systems that were in place they were able to identify what was happening. This is a good example of why organisations must not react to security breaches; instead they should be prepared for security breaches by identifying vulnerabilities, monitoring their systems and networks regularly and having controls in place (Cole, 2009). In order to protect networks properly there must be security controls in place and although it is impossible to eliminate all network security problems, such controls are nevertheless essential (Singh, 2009).

## 3.9 Security Controls

Security controls are mechanisms, policies and procedures that have the potential to reduce risk, respond successfully to attacks and improve security within the organisation. The term “controls” is often used synonymously with safeguards and countermeasures and refers to techniques that could be implemented to prevent, detect and respond to a security incident (Singh, 2009). Network security controls can be broken down into three types: physical controls, technical controls and operational controls (Photopoulos, 2011).

### 3.9.1 Physical Controls

Physical security controls consist of the security measures and devices that manage physical access to organisational resources. They are elements of the security infrastructure that reduce the effects of human abuse as well as the effects of acts of God. Physical controls include components such as standard keys, key cards, smart cards, identification badges, security cameras, motion sensors, audible and visual alarms, doors, locks, cages, fences and security guards. The way in which these components are put to use also determines the level of quality of the physical access control strategy (Singh, 2009).

Physical security is a type of security that ensures that no one can have access to physical resources without the proper credentials (Ballad et al., 2010). It includes the implementation, design and maintenance of controls that protect the physical resources of an organisation, including hardware, people and system elements. Important factors to consider when examining the physical security control include the following:

- What type of physical protection will be appropriate for buildings, office space, paper records or the data centre?
- Who holds the keys to what doors?
- What other critical areas exist in the building aside from the data centre and what is important about these areas?

### 3.9.2 Technical Controls

Technical controls are technical implementations of the security in the organisation; they are the components put in place in order to protect an organisation’s information assets. Technical controls consist of firewalls, routers, switches, VPN, antivirus software, intrusion detection and encryption techniques that focus mainly on protecting an organisation's ICTs and the information flowing across the networks (Baker & Wallace, 2007). They can be applied in many different ways, on a router port or protocol, and they are essential in enforcing policies for most of the IT functions, specifically those not under direct human control (Singh, 2009).

In addition, technical controls include logical access controls, such as identification, authentication, authorisation and accountability and the classification of assets and users (Whitman & Mattord, 2012). These are technology-based measures that manage logical access to information systems of the organisation (Photopoulos, 2011). Access control refers to a method for granting or denying an individual access to a restricted area of the organisation, such as a server room, or using specific resources (Ballad et al., 2010). It identifies who can interact with what and what that person is allowed to do during the interaction and is achieved through a combination of

- policies (rules governing the access to resources)
- procedures (nontechnical methods used to enforce policies)
- technologies (technical methods for enforcing policies)

When people are not cooperating or do not understand the reason for security controls, they may find ways to bypass the technical measures. Therefore, technology should not be considered in isolation from people, as people perform most of the procedures and operations in an organisation (Sasse, Ashenden, Lawrence, Coles-Kemp, Fléchais, & Kearney, 2007).

### 3.9.3 Operational Controls

Operational controls are the day-to-day procedures and mechanisms that are used for protecting the organisation's operating systems, applications and people (NIST 800-16, 1998) These are the policies, procedures and processes that define and guide people's actions and that restrict information resources. They are about the operations or actions that people in the organisation must perform to protect the information effectively. Operational controls include personnel security, physical security backup, contingency plans, recovery operations, system maintenance, off-site storage, user account establishment and deletion procedures (Baker & Wallace, 2007).

Even if technical and physical controls are implemented in an organisation network, if the operational controls are missing then they will serve no purpose. In order to protect the information of an organisation adequately all these controls must be in place. Indeed, physical controls are just as important as technical controls because if an attacker gains physical access to network devices even the technology-based controls may not be sufficient to prevent the attack (Ciampa, 2012). The IT management and IT professionals in an organisation are responsible for access security in technology equipment locations, and for the policies and standards that govern secure equipment operation. As with all the areas of security, the implementation of physical security controls, technical security controls and operational controls requires a policy. Such a policy is intended give users guidance on the appropriate use of the computing resources and information assets, as well as on protecting themselves (Ciampa, 2012).

## 3.10 Achieving Network Security

Organisations need to have multiple layers of security controls, policies, training and education and technology in order to present a strong network defence for network breaches. In achieving a secure network, the network security professionals must always be many steps ahead of anyone or anything that might compromise the security of the network; they must always remain aware of malicious activities and must have the skill to reduce the threats. They should attend training and workshops on security threats and have access to the latest security tools, protocols, techniques and technologies (Cisco, 2012). However, it is important that they do not neglect the network security policy which is essential for providing employees with guidance when performing their day-to-day work. An organisation is managing information security (network security) on the network adequately if the following exists (Singh, 2009):

- A network security policy that clearly defines the importance of network security for the organisation
- Clearly defined roles and responsibilities to ensure that all aspects of security are performed
- A security implementation plan describing the steps for implementing the policy
- The effective implementation of appropriate security hardware and software

- A plan to deal with any security breach that takes place
- A management review process to periodically ensure that security policies and standards are adequate, effective and enforced

## 3.11 Policy

A policy is a plan or a course of action which an organisation or business uses to influence and determine decisions, actions and other matters (Bacik, 2008). It is a high-level document, which represents the formal statement of the organisation’s managerial philosophy regarding its overall security (Whitman & Mattord, 2010). A security policy is a formal statement, which conveys the rules that people need to follow when they have been granted access to an organisation’s technology and information assets (Raval & Fichadia, 2007).

Policies are intended to give guidance to employees and partners of the company in aligning their actions and behaviour with that required by management (Von Solms & Van Niekerk, 2013). Policies generally direct how issues in the organisation should be addressed and how technology should be used (Whitman & Mattord, 2010). A policy should not specify the correct operation or function of equipment and software; this should be included in documents such as procedures, standards, practices and guidelines. A standard is a detailed statement of the things that must be done in order to comply with policy (Whitman & Mattord, 2010). Standards are the mandatory elements of policy implementation and include specifications and details on how a policy must be enforced (Singh, 2009).

For example, in implementing an inappropriate-use policy, an organisation can create a standard in terms of which all inappropriate content is blocked from the network and then list the material that is seen as inappropriate and also implement the policy technically. Procedures include the step-by-step instructions for implementing policies in an organisation, while guidelines are the recommendations related to a policy. Most organisations implement security by drawing up policies, standards, procedures and guidelines that specify the role played by users and administrators when maintaining the security of systems and networks (Singh, 2009). All these documents – procedures, standards and guidelines – give the detailed steps that are required in order to meet the requirements of a security policy.

The main purposes of a security policy are, according to Fraser (1997), to inform users, staff and managers of the compulsory requirements for protecting technology and information assets and to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with policies. The following section will focus on the levels of management in an organisation and the policies on each level.

## 3.12 Management Levels and Policies

There are three management levels that exist in an organisation, namely, strategic level, tactical level and operational level (Von Solms & Von Solms, 2006).

### 3.12.1 Strategic Level

The strategic level of management refers to the level where top management points out the importance of information assets to an organisation through the development of directives that outline the objectives of protecting information assets. At the strategic level top management is responsible for giving directives for the protection of critical organisational assets. Strategic level directives should be interpreted and communicated in related information security policies that dictate to the lower management levels how the process of information security should be interpreted and actually implemented (Von Solms, Thomson, & Maninjwa, 2011).

### 3.12.2 Tactical Level

The tactical level of management, in other words the senior and middle management, translates the directives from the strategic level in order to create policies and organisational standards and guidelines. The policies at this management level reveal the expectations of middle management regarding the protection of information assets.

### 3.12.3 Operational Level

The operational level of management, or the lower management and administration, translates the policies, standards and procedures from the tactical level into lower level policies, administrative procedures and administrative guidelines (Von Solms & Von Solms, 2006). Figure 3-3 below illustrates the relationship between these management levels and the documents related to each level. This diagram also shows how and where policies fit into the operations of an organisation

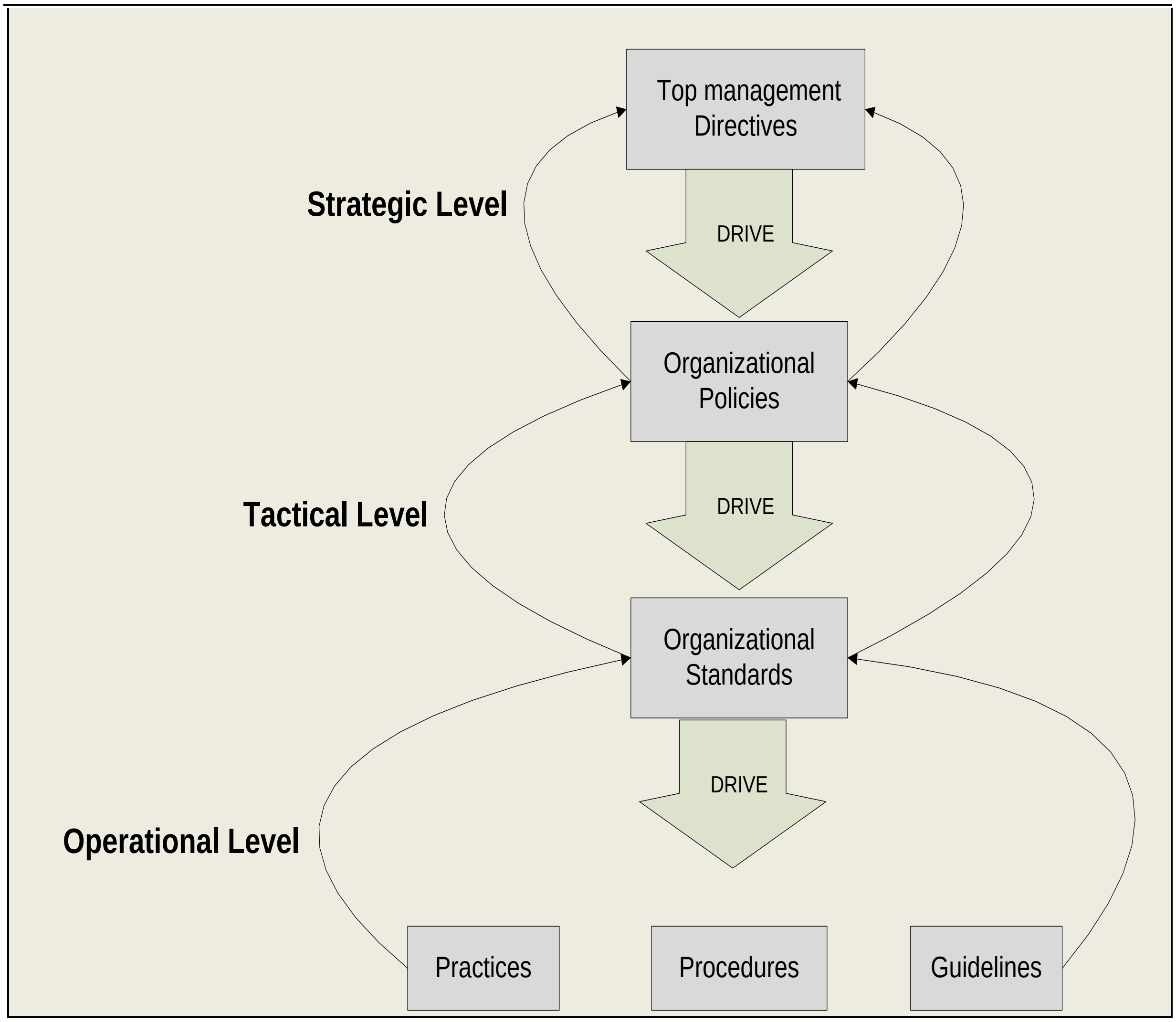

Figure 3-4: Management levels and policies (Whitman & Mattord, 2010)

The directives and policies that emanate from top management are generally contained in a structure called the information security policy architecture (ISPA). In fact, policies at each of the three organisational levels should form part of the organisation's ISPA. The ISPA consists of a set of documents, such as policies, guidelines and procedures, that structures the way in which the organisation protects its assets. An ISPA consists of documents which define the appropriate behaviour for asset usage, standardisation of tools for work and monitoring (Bacik, 2008).

In general, an ISPA is a representation of all the policies related to information security and it enables an organisation to remain abreast of the information security policies it has and how these policies are related to each other (Von Solms et al., 2011). The strategic directives of top management are important for the protection of information assets, as proper governance of information security is, to some degree, dependent on them. These directives are usually developed into various policy types and these will be discussed in the following section.

## 3.13 Types of Policy

There are three types of information security policy that must be defined in order to create a complete information security policy architecture (ISPA). The three types of policy are

- enterprise information security policies
- issue-specific security policies
- system-specific security policies.

### 3.13.1 Enterprise Information Security Policy (EISP)

An enterprise information security policy (EISP) is sometimes referred to as a corporate information security policy (CISP), a general security policy, an information security programme policy, IT security policy, a high-level information security policy, or an information security policy (Whitman & Mattord, 2010). It is the policy that sets the strategic direction, tone and scope for all the security efforts in the organisation. This includes assigning roles and responsibilities for the many areas in information security, such as maintenance of information security policies and the practices and responsibilities of end users. This is a high-level policy that must directly support the organisation's vision and mission statement. It is an important document that forms and moulds the security philosophy in the entire organisation. This type of policy may only require changes when the strategic direction of the organisation changes, otherwise it does not require frequent modification (Whitman & Mattord, 2010).

### 3.13.2 Issue-Specific Security Policy (ISSP)

An issue-specific security policy (ISSP) focuses on addressing specific areas and providing more detailed or targeted guidance for people in the organisation about the use of a system, technology or processes. It conveys the expected usage of the specific technology-based systems of an organisation and is intended to act as a standard for compliance. It also contains procedural elements and an issue statement that gives detail about how the organisation views a particular issue. It is more detailed than an EISP and requires frequent updates. An ISSP may cover topics such as the use of the Internet and the World Wide Web, the use of electronic mail, disaster planning and/or business continuity planning, and the use of personal equipment on company networks (Whitman & Mattord, 2010).

### 3.13.3 System-Specific Security Policy (SysSP)

A system-specific security system (SysSP) is a type of policy that functions as set of standards or procedures to be used when configuring or maintaining systems. A SysSP can be divided into managerial guidance and technical specifications. For example, a document for configuring and operating a firewall could include a statement of managerial intent, guidance for network engineers on selecting, configuring and operating firewalls, and an access control list that defines levels of access for each authorised individual. A few of the most important rules that should be followed during the creation of policies are the following (Whitman & Mattord, 2010):

- Policy must never conflict with the law – having a policy that conflicts with the law constitutes a criminal act.
- Policy must be able to stand up in court if it is challenged.
- Policy must be appropriately supported and administered.

It is the responsibility of top management to ensure that the organisation complies with all the applicable country and industry laws and regulations, as well as with all organisational directives, policies, standards and procedures.

## 3.14 Importance of Policies

Policies help in documenting the expected behaviour of employees in order for them to understand the type of behaviour that is required from them and the consequences of violating that behaviour (Bacik, 2008). Employees who do not comply with security policies could be a key threat to the security of the organisation's network (Siponen, Mahmood, & Pahnila, 2014). Organisations facing security threats to their assets must have security policies which direct the way in which the assets are to be managed and protected (Ahmed et al., 2012). When an organisation has policies in place it does not mean that employees will automatically obey these policies. Therefore, to ensure appropriate behaviour, these policies should, ideally, become part of the organisational culture (Von Solms & Von Solms, 2004). Organisational culture can be seen as the attitudes, values, beliefs, norms and customs of an organisation; it can also be seen as a pattern of assumptions that may have worked in the past and is still considered valid (Lacey, 2010). Changing the way people conduct themselves in an organisation demands a good understanding of human behaviour and is one of the hardest challenges, as it requires careful attention to human factors.

## 3.15 Human factors

The human factor is about people. It is concerned with people in their working and living environment, and their relationships with equipment and procedures as well as the people around them. The human factor is an element that influences the way people behave when carrying out a certain function (Licht, Polzella, & Boff, 1989). Furthermore, the human factor focuses on the nature of human interaction; it deals with understanding human interaction and other elements of the system in order to achieve human well-being and overall system performance (Salvendy, 2012). For example, entering the wrong value on a form, deleting the wrong file or pulling out the wrong plug by mistake. Little mistakes like these are the very nature of being human; these are the human aspects or characteristics of being human (Hinson, 2014). In the case of network security, configuration mistakes made by careless employees could leave network ports open, firewalls vulnerable and entire systems completely unprotected (Ahmed et al., 2012).

Every day many organisations or business information systems and networks face security threats from diverse sources such as computer fraud, computer hacking, malicious code, fire or flood (ISO/IEC 27002, 2007). Most of the techniques used by attackers and hackers to compromise networks or IT systems demonstrate that the human element is often crucial for the success of attacks (Ahmed et al., 2012). In other words, these attacks take place as a result of human involvement despite the implementation of technological security in networks or IT systems.

It does not matter how many technical security solutions, such as firewalls, antivirus programs and encryption, are implemented on the network of the organisation, if the human factor is neglected then these solutions will be useless (Gonzalez & Sawicka, 2002). According to Gonzalez and Sawicka (2002), the human factor is the Achilles heel of information security; as technology advances even further, employees play an important role in the success of any company and yet they are often the weakest link when it comes to information security and network security. This means that security systems rely on people; no matter how well designed or well implemented they are humans play a crucial role and are the most challenging part of security (Huang, Patrick Rau, Salvendy, Gao, & Zhou, 2011). It is therefore important to ensure that security systems (networks) depend not only on the technical aspects, but also on the people that use the systems (Alavi, Islam, Jahankhani, & Al-Nemrat, 2013).

People are the most important resources in most organisations and they perform all the physical and cognitive tasks, such as inspecting components, issuing tools, entering data and managing people and operations (Lehto & Landry, 2013). However, the people that use the systems and networks vary when it comes to behaving securely and are consequently difficult to control. People are not perfect and will always be prone to make mistakes (Ahmed et al., 2012).

### 3.15.1 Human Error

When people use any system mistakes are bound to happen, owing to the complex way in which people think and the other influences that affect them. These influences can be external (organisational environment) and internal (individual’s private life). Consequently, there will always be the possibility of an individual making a mistake (Ahmed et al., 2012).

These mistakes may be the result of improper training, lack of experience, lack of supervision, lack of concentration and possible negligence. An employee’s negligence can create vulnerabilities and opportunities for criminals to steal, manipulate and corrupt information assets by, for example, clicking an “ok” button without actually reading the error message or neglecting to follow proper security policies and procedures.

An organisation’s employees could be its greatest threat, since their mistakes could present a threat to the confidentiality, integrity and availability of information. Employee errors could lead to (Whitman & Mattord, 2012)

- the exposure of confidential information
- the entry of incorrect data
- the accidental deletion or modification of data
- the storage of data in unprotected areas
- a failure to protect information.

There are two types of human error, accidental and deliberate. Accidental causes are unintentional and non-deliberate, for example an accidental programming error that causes a computer to crash under certain circumstances (Kraemer & Carayon, 2007). Deliberate errors on the other hand, such as insider threats, seek to do damage deliberately (Council National Research, 2002).

An example of an insider threat would be a disgruntled employee who is determined to do harm and who has some technical skills to accomplish that (Cisco, 2012). Disgruntled employees are the major source of targeted computer attacks, with many cases having been reported (Cardenas, Amin, Sinopoli, Giani, Perrig, & Sastry, 2009). For example, on 10 December 2007, Chan, a disgruntled former employee, pleaded guilty in the United States federal court to unauthorised access of a company computer that caused $5000 worth of loss to the company. Chan, a former employee of the Loves Park Company, had worked in the IT department. After the termination of his employment with the company in 2005 he started accessing the company’s computer system. He then started accessing computer files, changing prices on customer invoices and deleting customer files. The company network was significantly slower when all these transactions were taking place and the company spent over $10 000 restoring the integrity of the system (FBI, 2007). Organisations usually have controls in place that detect when an outsider (non-employee) tries to access organisational data and they have a way of mitigating or reducing the threat of an outsider. In contrast, the perpetrator who is harder to detect and who can often cause the most damage is the insider (FBI, n.d.).

Inside threats to the organisation may consist of people working for the organisation and outside contractors with insider access. However, firewalls and security tools may be inadequate in preventing network attacks such people (Snedaker, 2006). Many organisations are still old fashioned in their outlook, only protecting their information assets and networks from those outside the organisation (Jones & Colwill, 2008). It should be borne in mind that people working for the organisation have the potential to do great harm because they know the processes and procedures and the location of high-value assets in the organisation.

The attacks carried out by people within an organisation can be driven by motivation, opportunity and capability. The motivation can be a result of internal, personal drivers, whereas opportunity and capability can be achieved once the individual is inside or working for the organisation (Jones & Colwill, 2008). It is important that human factors be given serious attention by organisations, as human error in the failure to secure the network can be prevented with training, ongoing awareness activities and controls such as procedures that include the verification of commands by a second party or forcing the user to type critical commands twice (Council National Research, 2002).

### 3.15.2 Human Behaviour

If the organisation is to be effectively secured then human factors must be given adequate attention because they have to potential to become uncontrollable (Alavi et al., 2013). For example, people carry out various organisational tasks during which they may work individually, in a group, or with management and customers or suppliers that could have a different perception or view of security. The way users react to security procedures will vary from person to person as each has his or her own concerns, values, culture, skills, knowledge, attitudes and behaviour when it come to making security decisions (Alavi et al., 2013).

Human behaviour plays a crucial role in most security failures. Security breaches in organisations that are caused by employees could be the result of ignorance of the security policies or negligence (Vroom & Von Solms, 2004). The behaviour of employees, whether intentional or through negligence, is often due to a lack of knowledge (Van Niekerk & Von Solms, 2010). According Van Niekerk and Von Solms (2010), the human factor in information security has two dimensions, namely, knowledge and behaviour. Accordingly, just as the employee requires knowledge of information security practices to perform a certain job function, so network administrators require knowledge of network security practices when configuring and maintaining the network devices.

It should not be assumed that the average employee has all the knowledge required to perform his/her job in a secure manner. An organisation needs to cultivate a security aware culture or an information security culture (Van Niekerk & Von Solms, 2010). An information security culture can be described as the way things are done in an organisation, including the attitudes, assumptions, beliefs, values and knowledge that employees bring into play when interacting with the organisation's systems and procedures at any point in time (Veiga & Eloff, 2010). In other words, for employees to perform their day-to-day activities in a secure manner they must have sufficient knowledge of information and network security practices (Van Niekerk & Von Solms, 2010). It important that employees are made aware of both acceptable and unacceptable behaviour when at work; in other words there have to be guidelines for directing their behaviour and establishing accountability for their conduct. If employees have no guidelines or rules they will form their own view of what is allowed and not allowed, which could make it hard for employers to maintain security and take disciplinary action when necessary. Clear guidelines are needed in order to emphasise acceptable behaviour and the penalties for not engaging in that behaviour (Colwill, 2009).

The use of technologies like firewalls and intrusion detection systems provides some form of protection for networks and applications. However, network administrators can make serious mistakes when configuring network devices, which could eventually result in greater security problems. Improper configuration of networking devices can lead to serious network vulnerabilities and threats such as flooding attacks and insecure transmission (Hamed & Al-Shaer, 2006). However, the erroneous actions and behaviour that employees engage in are the biggest threat to the success of both information security and network security. In order for this threat to be reduced employees need to learn and incorporate acceptable security practices into their everyday behaviours (Thomson, Von Solms, & Louw, 2006). When it comes to behaving in a secure manner the culture of the organisation plays a huge role – it influences the mindset of each individual which can ultimately change their actions with regard to security (Deloitte, 2009).

### 3.15.3 Organisational Culture

In each and every organisation there is an organisational culture. This culture may be well known or unknown to the people in the organisation (Thomson et al., 2006). According to Lundy and Cowling (1996), organisational culture can be defined as “the way things are done here”, in other words the organisational routines and rituals or procedures for doing things (Lundy & Cowling, 1996). Furthermore, organisational culture could be viewed as the personality of the organisation or the glue that unites the people in the organisation (Kreitner & Kinicki, 1995).

This culture shapes and influences the way employees conduct themselves when it come to securing the information assets of the organisation. It is very important that every organisation has a balanced organisational culture as it establishes the way employees should behave (Thomson et al., 2006). The organisational culture should include information security as a subculture in order to properly influence employees to behave in a secure manner.

The establishment of organisational information security as a subculture is key to managing the human factors involved in information security (Van Niekerk & Von Solms, 2010). As mentioned previously, an information security culture can be described as the way things are done in the organisation as regards security, including the attitudes, assumptions, beliefs, values and knowledge that employees display when interacting with the organisation’s systems and procedures at any point in time (Veiga & Eloff, 2010). The information security culture could bring changes to the way employees behave towards security, could make them more security aware and could influence them follow good security practices when performing their everyday activities (Colwill, 2009).

Changing the way employees behave requires breaking old habits and creating new ones through security training (Sasse et al., 2007). Many researcher agree that employees are generally viewed as the weakest link in the organisation's security chain (Ahmed et al., 2012; Monk, Van Niekerk, & Von Solms, 2010; Deloitte, 2009; Ernst & Young, 2008). However, the same employees could be the strongest link in the security chain, if employees could be adequately trained to protect the information assets of the organisation (Thomson et al., 2006).

An information security culture develops as a result of the information security behaviour of employees. The same can be said for organisational culture – organisational culture develops because of employees' behaviour in the organisation. When cultivating an information security culture, the organisational culture should be considered to ensure that the most appropriate controls are identified and deployed in a successful and effective manner (Veiga & Eloff, 2010).

### 3.15.4 Organisational behaviour

Once the security culture of the organisation is understood, the behaviour of employees will start to adapt to security consciousness behaviour. Organisational behaviour occurs on three levels and each level is affected by different factors. The three levels of organisational behaviour are (Vroom & Von Solms, 2004) the following:

- The individual
- The group
- The formal organisation

Individual behaviour includes all the unique characteristics of each person such as an employee's attitude, personality, motivation and job satisfaction. In the development and evolution of the organisational culture, the behaviour of the individual plays an important role and should contribute to information security. The behaviour of the formal organisation is influenced by the environment around it which influences its employees and internal operations.

These levels of organisational behaviour influence each other and together form the culture of the organisation. Each of these organisational behaviours comprises a unique type of behaviour, because the way individuals act differs from the way that the group that these individuals belong to reacts in situations. For the culture of the organisation to change, it has to be changed on all these of three levels. For example, by influencing the group to become more security conscious, the organisation as a whole would benefit and therefore the culture would incorporate information security in everyday routine. When changing the culture of an organisation it may be valuable to incorporate security behaviour into the employees' routine. Accordingly, the security culture should be aligned with the organisation's security policies (Vroom & Von Solms, 2004).

The security behaviour of employees is not a command and control approach but rather an understanding of what it means to behave securely (Sasse et al., 2007). The best non-technical measures available to address the human factor and security are security education, security training and security awareness; hence they should be used to create a proper understanding of the threats facing information systems and how people should behave in the face of them (Jones & Colwill, 2008; Colwill, 2009). employees of the organisation (whether IT professionals or not) need to learn to think and act in a security conscious way (Sasse et al., 2007); therefore the key to addressing the human factor in an organisation is through security awareness, training and education (NIST 800-16, 1998).

## 3.16 Security Education, Training and Awareness

When the organisation has properly identified the policies that will guide its security programme and has chosen an overall security model, the implementation of the security education, training, and awareness (SETA) programme can then follow. A SETA programme is intended to decrease the security breaches that occur as a result of a lack of security awareness in employees (Hight, 2005) and the goal of such a programme is to improve employee awareness of the need to protect system resources and to develop skills and knowledge of secure behaviour when performing their jobs.

The implementation of a successful SETA programme forms part of managing the risk in the organisation because uneducated employees could pose a huge risk that could jeopardise the security of the entire organisation (Whitman & Mattord, 2012). According to Wood (2002), a SETA programme could create a “human firewall” which could be more powerful than correctly configured firewalls and intrusion detection systems. If people in the organisation are aware and adequately educated, they could form a layer of protection similar to a firewall with the potential to prevent and identify threats to the organisation’s information assets.

As previously stated, technology alone will not solve security problems. It is therefore important that employees are security aware, and have been trained to act as a “human firewall” in the organisation (Wood, 2002). The elements of a SETA programme (security education, training and awareness) will be further discussed in the following section. The following section presents a security-learning continuum model from the awareness stage through training and then education. It also includes the concepts associated with each learning level.

### 3.16.1 Cyber Security Leaning Continuum Model

In order for people to perform their roles in an organisation, specific tools and training are required. Such tools and training can include basic security awareness, education, experience and the knowledge, skills and ability appropriate for their roles. The National Institute of Standards and Technology Special Publication 800-16 (2013) has designed a model called the Cyber Security Learning Continuum to help organisations in providing the correct tools and training for their employees (NIST 800-16, 2013).

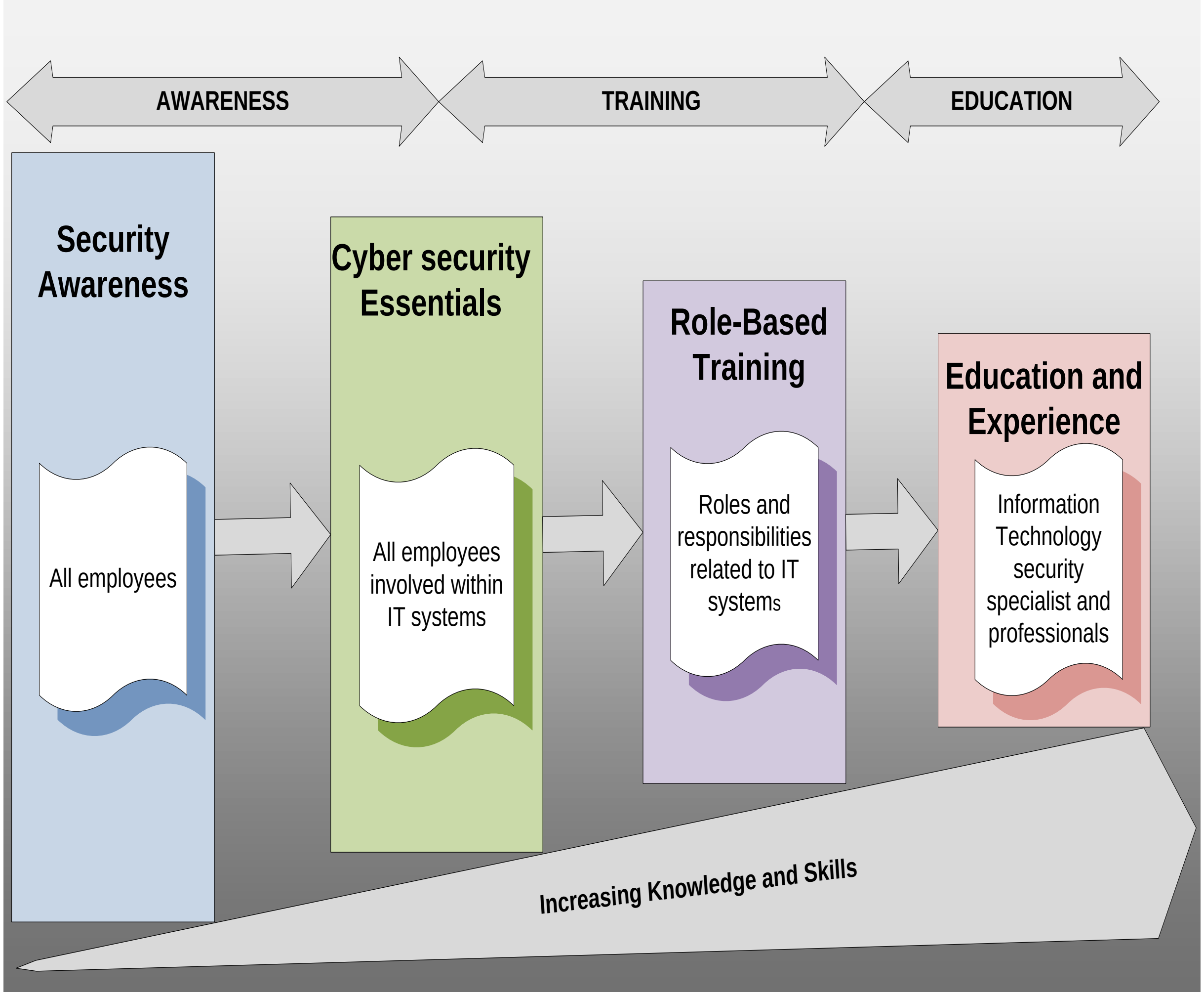
AWARENESS
TRAINING
EDUCATION
Security Awareness
All employees
Cyber security Essentials
All employees involved within IT systems
Role-Based Training
Roles and responsibilities related to IT systems
Education and Experience
Information Technology security specialist and professionals
Increasing Knowledge and Skills

Figure 3-5: Cyber Security Learning Continuum Model (NIST 800-16, 2013).

The model illustrated in Figure 3–5 is built on the principle that learning is a continuum. In other words, learning is a continuous process; it starts with the awareness stage, moves to training and then education (NIST 800-16, 2013). The Cyber Security Learning Continuum illustrates the relationships between security awareness, cyber security essentials, training and education. It also demonstrates that awareness and training form the foundation necessary for all individuals that use IT systems and/or are involved in management and maintenance in the organisation. It also demonstrates that role-based training and education is provided selectively, according to an individual's responsibilities and needs. In other words, network security or cyber security training is provided to people on the basis of their specific roles and responsibilities with regard to the organisation's information systems (NIST 800-16, 2013).

For example, John is a network administrator in an organisation. As an employee of the organisation, John needs to attend the annual security awareness training. He is also in the IT department, so he receives additional training on cyber security best practices, known as cyber security essentials. In his role as network administrator, John has significant IT (network) responsibilities and is therefore required to attend role-based training. The following sections will discuss the concepts illustrated by the model further together with the related SETA elements.

#### 3.16.1.1 Security Awareness

Security awareness is the start of the security learning process, the purpose of this level of learning is to allow employees of the organisation to recognise IT security concerns and security issues and to inform users about how they should respond to them (Koroliov, Turesson, & Brolin, 2009). The word “users” refers to employees, contractors, visitors and other co-workers or associates requiring access to information systems (network of the organisation) (NIST 800-16, 2013).

In security awareness the learner is the receiver of information. Awareness relies on reaching broad audiences and includes programmes such as security newsletters, security posters, flyers and security slogans printed on coffee cups or T-shirts (Sasse et al., 2007). It is very important that the organisation motivate its employees have a desire for security. In addition, the employee must know what should be protected in the organisation, such as the critical information assets.

#### 3.16.1.2 Cyber security Essentials

Cyber security essentials form a level of learning that is required for all the employees of the organisation, including the contracted employees, who are involved with IT systems. This is a transitional stage between basic awareness and role-based training and provides the foundation for a role-based training programme. The term “cyber security essentials” refers to an individual’s ability to apply the knowledge needed to protect electronic information and systems. Everyone who uses computer technology or the output products of technology, whatever their specific job responsibilities, must know these essentials and be able to apply them (NIST 800-16, 2013).

#### 3.16.1.3 Role-based Training

Individuals may take different roles in the organisation based on their individual skills. Some examples of roles include network administrators, system administrators, information assurance technicians, information assurance managers and cyber security managers (Whitman & Mattord, 2010). Each role has associated competencies, in other words there are skills and knowledge that the individual occupying the role has to have. A role-based security training curriculum might not necessarily result in a formal degree from an institution of higher learning; however, it may contain similar material to that found in a certificate or degree programme at a college or university.

This learning level is more formal than the awareness and cyber security levels of the learning model. It is intended to help personnel understand and improve their performance of their specific security role and consequently protect the organisation's information systems. It is important that in the organisation training is specifically available for the people responsible for information and network security or IT systems. It does not really matter whether the training programme is developed within the organisation or by a training company, just as long as there is some form of training available (NIST 800-16, 2013).

#### 3.16.1.4 Education and/or Experience

Education that takes place in the advanced stage of security learning relates to the completion of formal education such as degrees and graduate studies in the fields of IT security or network security. Such education can include industry-recognised IT security certification as well as programmes offered by higher education institutions. It further focuses on developing the ability to perform complex multidisciplinary activities and the skills needed for information technology or network professionals. This education is necessary because these professionals must be up to date when it comes to threats and technology changes. The education stage combines or integrates the experience that the individual has gained on the job and training through certificate or degree programmes. The form of learning on this level becomes broader and more detailed, as depicted by the increasing knowledge and skills in the Figure 3–5 (NIST 800-16, 2013).

## 3.17 Conclusion

This chapter examined the various security domains and their associated concepts. Security is an unending continuous process; consequently it is impossible to completely eliminate all security problems. In addition, the large number of security threats facing the network and information systems, could put the organisation’s reputation and revenue at risk. Despite the presence of properly configured network devices and technologies, organisational networks could still be susceptible to attacks as a result of human vulnerabilities – networks are configured and maintained by humans, humans make mistakes and thus have limited accuracy and attention. In this chapter it was argued that addressing the human factor specifically in network security is of the utmost importance, as networks are the foundation of most business processes.

This chapter further explored the importance of having multiple layers of security controls, such as policies, education, training and awareness and technology, in order to address the human factor in the network. To have a strong network defence, the human factor must be addressed and a security culture cultivated in order to encourage people in the organisation to behave securely when performing their jobs. In this chapter emphasis was placed on understanding the human factor in network security as well as the way in which the human factor is addressed in organisational networks. The following chapter will explore the National Research and Education Networks (NREN), the importance of and the roles played by NRENs in various countries, will further explore the South African NREN known as SANReN.

# CHAPTER 4: NRENs AND SANReN

## 4.1 Introduction

*"National governments should be aware that research and education networking in their country, and in particular their National Research and Education Network organisation (NREN), is an asset for economic growth and prosperity. It is a source of innovation and provides fast and widespread technology transfer to society and industry" (Dyer, 2009).*

Network connectivity is the key enabler of collaboration, and without it research, education, and society would not function properly (ASPIRE, 2012). Researchers all over the world are on a quest for collaboration on and participation in global knowledge through the network connectivity of NRENs (TERENA, 2012). This chapter explores the South African Research and Education Network (SANReN). The SANReN is a type of National Research and Education Network (NREN) and is a subset of the Research and Education Network (REN), which extends over multiple countries. Therefore, this chapter will briefly introduce the concept of RENs, as well as discuss the benefits and services provided by NRENs. Thereafter the focus falls onto the SANReN.

## 4.2 Research and Education Network (REN)

The Research and Education Network (REN) connects the computer networks of research and education institutions in order to assist in information exchange for research and teaching purposes. RENs have played a significant role in the development of the Internet, as they were part of the first users of computer networks.

Europe has become the world leader in RENs; consequently many regions in the world are following the example of Europe when designing or establishing their RENs. Figure 4-1 below depicts an organisational model of a single NREN in a country in Europe. It demonstrates the types of network that can be connected directly to an NREN, such as the Local Area Network (LAN), Metropolitan Area Networks (MANs) and regional networks. It also shows how RENs connect to the Internet. The structure of this European model has been copied in other regions of the world.

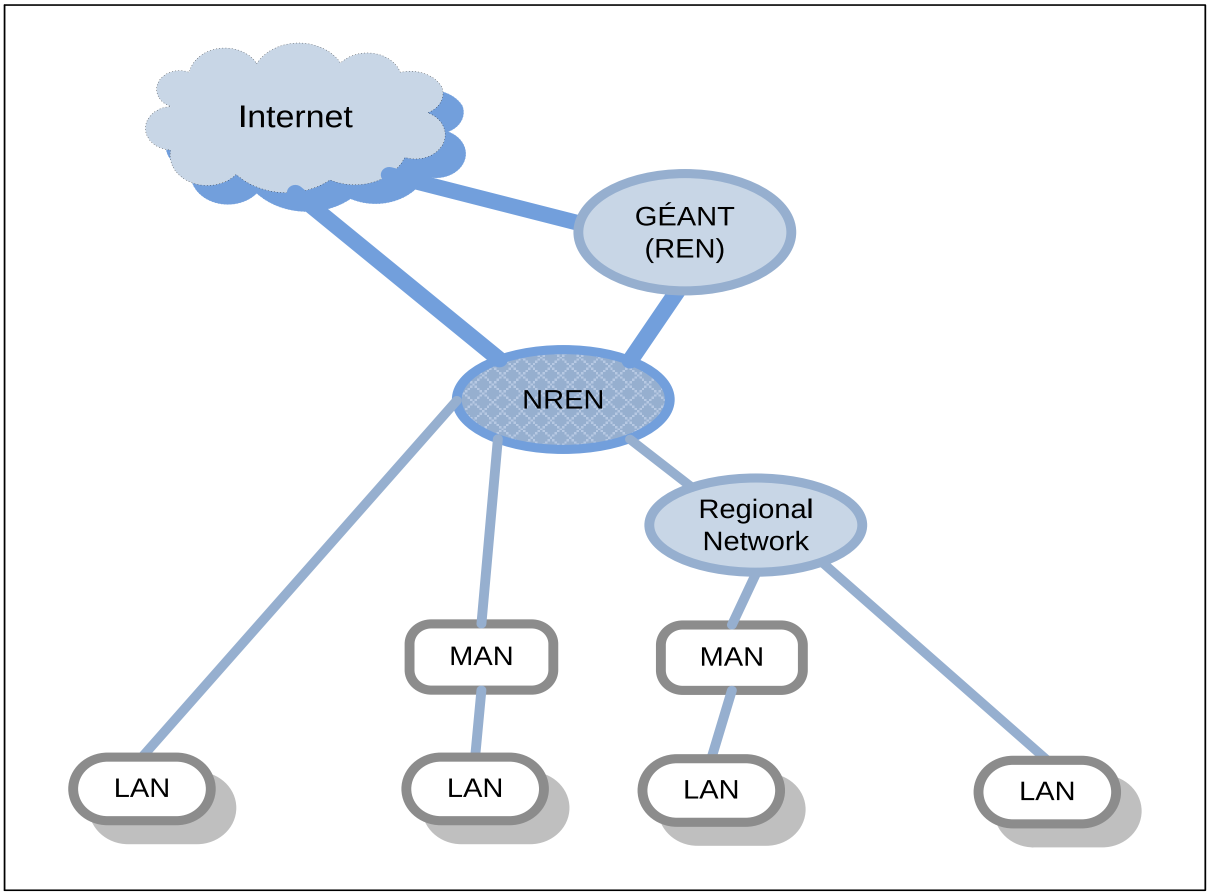

Figure 4-1: Structure of RENs in Europe (Dyer, 2009)

Furthermore, RENs can exist on two levels: on the local (national) and the regional (international) levels (TERENA, 2010).

### 4.2.1 Local REN Level

The network interconnecting the local networks is on the national or local level. This national level is responsible for the National Research and Education Networking organisation, that is, the NREN of a country. In most countries, the local Research and Education Networks are formally known as the NRENs (TERENA, 2010), and these will be discussed in section 4.3. NRENs interconnect the local networks of the research and educational institutions of a country (as shown in Figure 4-1).

### 4.2.2 Regional REN Level

On a regional or international level, there are continental networks such as GÉANT that interconnect NRENs in certain regions of the world. GÉANT stands for Pan-European Research and Education Network and it interconnects Europe's NRENs (TERENA, 2013). The GÉANT network is a global centre for research networking; it connects research and education communities within Europe and with other regions of the world such as North America, South Africa, Central Asia, North Africa and the Middle East. The GÉANT project is collaboration between 41 partners: 38 European NRENs, DANTE, TERENA and NORDUnet.

Furthermore, this network connects over 50 million users at about 100 000 institutions across Europe and, through the GÉANT network, over 100 countries around the world are currently interconnected with high-speed links, which are dedicated to research and education. The GÉANT network provides the international connection between NRENs, and DANTE manages these connections on behalf of the NRENs. DANTE is an organisation that operates and manages the European NRENs. The name DANTE stands for Delivery of Advanced Network Technology to Europe (Dyer, 2009). The GÉANT is co-funded by the European Union (EU) and European NRENs (TERENA, 2013). Connectivity to the Internet can take place both at the NREN level and, to some extent, at the GÉANT level.

## 4.3 National Research and Education Network (NREN)

As mentioned in section 4.2.1, NRENs are National Research and Education Networks. They are responsible for the provision of data communication networks and services to the research and education community in a country (DANTE, 2014). In other words, NRENs are specialised Internet service providers for the research and education communities in a country, providing services and access to the Internet to these institutions, and support for colleges, schools, libraries and other public institutions. A Country usually has at least one NREN, although in large countries it is common to have more, with separate regional or local NRENs.

The ownership and funding model of the NREN varies from country to country. In some countries NRENs are owned by the government or by the institution that receives the REN services, or a combination of both the institution and government (TERENA, 2013). Furthermore, some or all the operational costs may be funded by the government, or the institution receiving the services may finance some or all the operational costs (TERENA, 2010).

Developing and operating an NREN is not a simple task, as it requires careful planning and an understanding of the changing IT environments (TERENA, 2013). The day-to-day functions of the NREN can be undertaken by dedicated NREN staff, or staff of a member institution, or outsourced to an external organisation. The availability of skilled staff, levels of funding and commercial agreements usually determine who will manage and operate the NREN (TERENA, 2010). The staff providing network connectivity and services plays a crucial role as the first link in the networking chain. It is thus important for local IT staff at the NREN participating institutions to understand the needs of users and help them to use services effectively (Dyer, 2009).

As mentioned in section 3.11, if people have no guidelines or rules that govern their behaviour they will form their own view of what is allowed and not allowed, which could possibly make it harder to maintain the security of the network (Colwill, 2009). As clear guidelines on acceptable behaviour are important, NRENs have policies in place that should be implemented to govern the network usage. These policies include, but are not limited to, a Connection Policy (CP), an Acceptable Use Policy (AUP) and Statues and Articles of Association. These documents specify how the NREN network should be connected, as well as what is allowed and not allowed on the network. These policies are particularly important for network usage because NRENs connect a variety of communities such as research centres, universities, schools, museums, hospitals and government departments (ASPIRE, 2012).

NRENs play a big role in connecting countries and thus have a special position in the research community (Dyer, 2009). They generally operate as non-profit organisations for a particular group of users and control carefully whom they deliver their services to, unlike the commercial ISP (Jaume-Rajaonia et al., 2003). The first implementations of Internet innovations are, typically, on NRENs and later extend to the commercial ISPs. NRENs do not compete with commercial ISPs, but have as their mission the offering of a different level of service; hence, they provide a platform for encouraging and conducting research in high speed networking (SANReN, 2012).

One of the biggest differences between NRENs and commercial ISPs is the fact that an NREN is part of the research and education community and thus have a thorough understanding of both their users' expectations and requirements. Further, unlike commercial ISPs, NRENs are not motivated by profit-making (ASPIRE, 2012). Commercial ISPs have no motivation to accomplish the level of innovation required by the education and research community (Dyer, 2009).

### 4.3.1 NREN Services

NRENs normally provide high-speed, high-capacity infrastructure together with advanced services that often are not found elsewhere on the Internet, such as eduroam. Eduroam is a secure worldwide roaming access service that has been implemented for the international research and education community. It allows researchers, staff and students at participating universities to obtain Internet access on their 'home' campus and when visiting other participating universities. Eduroam is available in 66 countries, but having eduroam in a country does not mean that it is available in all institutions, only those institutions that are part of the NREN of the country (TERENA, 2013).

Other services that NRENs provide include media streaming, videoconferencing, IP telephony, access federations and wireless roaming. The lowest capacity for an NREN connection is 1 GB/s, however, most European NRENs and other NRENs have 10 GB/s and above as their capacity. Many regions now have access to dark fibre which enables them to have high capacities (TERENA, 2013). Some NRENs have already upgraded their backbones to 100 Gbps. It is important that NRENs provide services that are unavailable on the commercial market, as basic services such as email, spam filtering and so on may already be available on the market at low cost.

### 4.3.2 Collaboration between NRENs

NRENs are at different levels of maturity in their development, with some being more mature than others. Small NRENs in developing countries rely on the collaborative nature of the NREN community for expertise, training, the provision of best practice guides and the provision of services by other NRENs (ASPIRE, 2012). It is important that the more mature NRENs collaborate and assist developing NRENs. NRENs of continents or regions should strive to work together and collaborate with each other. Eduroam, as discussed in section 4.3.1, is a good example of the successful collaboration between NRENs (ASPIRE, 2012).

NRENs have become the underpinning foundation not only of cyber infrastructure; they are also the platform that other cyber infrastructure components and services rely on. Therefore, it is important that national governments are aware that the NRENs in their country are assets for economic growth and a source of technological innovation (Dyer, 2009). In South Africa, the national research network is known as SANReN. The following section will focus on the South African NREN.

## 4.4 South African NREN (SANReN)

SANReN is a high-speed communication network that is designed primarily for research institutions and organisations in South Africa. The SANReN network was deemed a suitable case example for this research, as it is a relevant example within the South African context for emphasizing the importance of addressing the human factor.

The regional REN for SANReN is UbuntuNet Alliance. UbuntuNet Alliance is an organisation that functions as a regional REN for Eastern and Southern Africa. Its purposes is to provide NRENs with regional and global interconnectivity with other NRENs and with the Internet (Martin, 2012). In other words, the UbuntuNet Alliance is the regional REN connecting SANReN with other NRENs and with the Internet. Figure 4-2 below demonstrates the hierarchy or order in which these organisations are connected from national level to international level (these levels are discussed in sections 4.2.1 and 4.2.2).

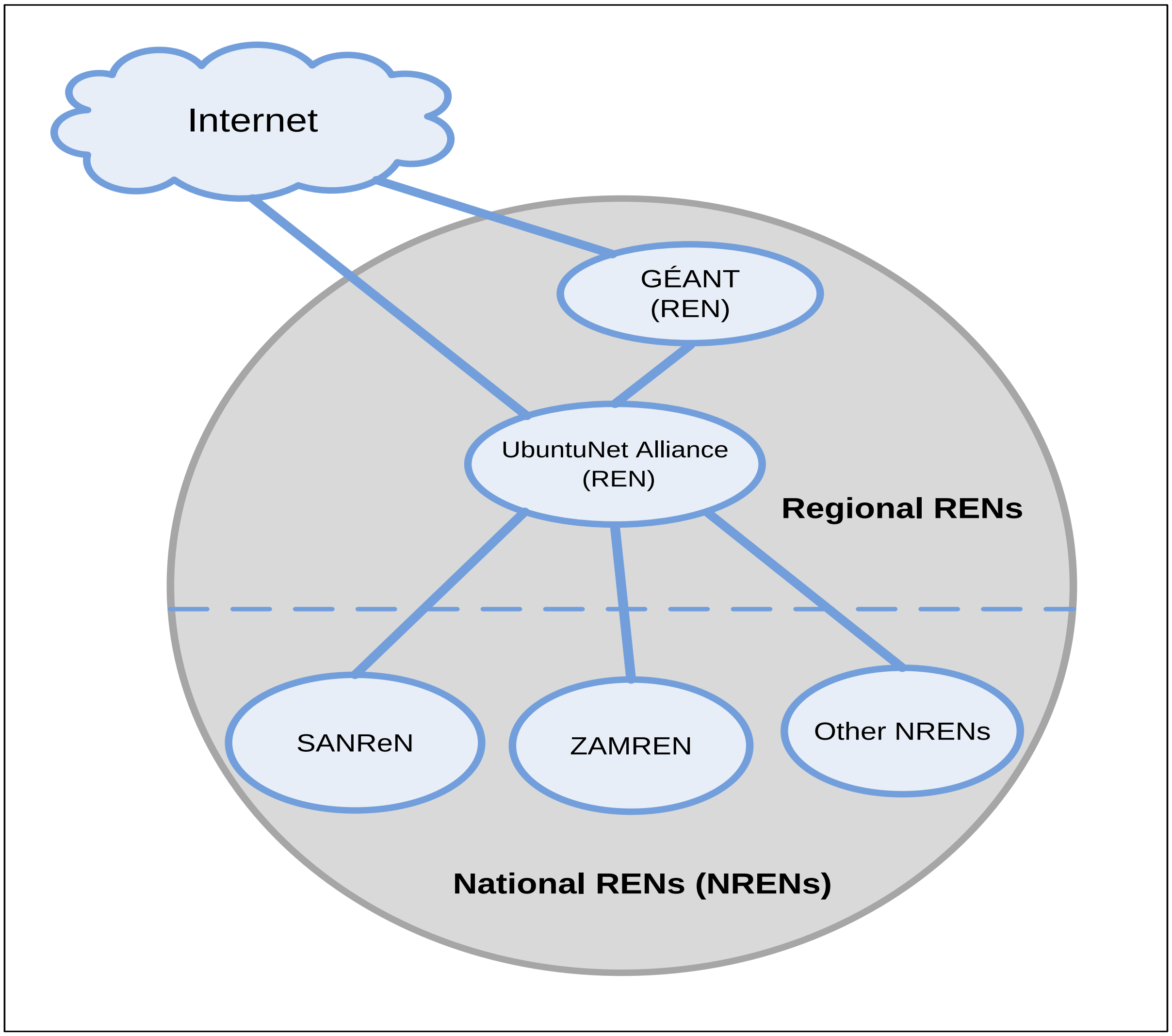

Figure 4-2: Structure of RENs in Eastern and Southern Africa (Martin, 2012)

In addition, Figure 4-2 shows how the SANReN connects to international NRENs and the Internet through the UbuntuNet Alliance PoP (Martin, 2012), as well as how SANReN connects with other NRENs in the Eastern and Southern African regions, such as ZAMREN which is a Zambian NREN.

The main purpose of the SANReN network is to provide South African research institutions and organisations with Internet access and related services, as well as connecting them to research networks all over the world. The SANReN network, together with the Centre for High Performance Computing (CHPC) and Very Large Databases (VLDB), create the key components of the cyber infrastructure in South Africa (Meraka Institute, 2007).

The major role players of the SANReN network are

- Department of Science and Technology (DST)
- Council for Science and Industrial Research (CSIR) Meraka Institute
- Tertiary Education and Research Network of South Africa (TENET)
- SANReN beneficiary institutions

The SANReN network is a South African DST project, implemented by the CSIR through the Meraka Institute (Meraka Institute, 2007). The project was conceptualised in 2003 and forms part of the South African government's approach to cyber infrastructure and to ensure the successful participation of South African researchers in global knowledge (SANReN, 2014). The CSIR is the governing body of the SANReN network and the operational services of the SANReN network are provided by TENET to all beneficiary institutions on behalf of the CSIR (SANReN, 2014).

A SANReN beneficiary institution is an institution that is defined by the DST as an institution that is allowed to be connected to the SANReN network. These beneficiary institutions are the current TENET institutions, and include the South African universities, research councils such as the CSIR, the National Research Foundation (NRF) , and various other research institutes (SANReN, 2014). The following subsection will provide more detail on TENET as one of the SANReN role players.

### 4.4.1 TENET

TENET is a specialised ISP for the higher education and research sector, which provides Research and Education Networking services to about 160 campuses of 54 institutions, including universities, research councils and other associated institutions (UbuntuNet Alliance, n.d.). All the public universities and science councils in South Africa qualify to be a part, or a member, of the TENET network (Martin, 2012). TENET represents the institutions' interest, while SANReN represents the South African government's interests (SANReN, 2012). The roles and responsibility of the South African NREN (SANReN) are distributed between the SANReN team and the TENET team. The SANReN team builds the network and the backbone connectivity and develops innovative services. The TENET team on the other hand is responsible for operating the network (Martin, 2012).

The TENET team is based in Cape Town and Johannesburg and has about 12 full-time staff, while the SANReN team is situated at the CSIR Meraka Institute in Pretoria as a sub-unit reporting to the DST through the CSIR Executive Director (SANReN, 2012). The SANReN project is funded by the DST and currently consists of 15 full-time staff. According to the SANReN management, SANReN staff (SANReN engineers) have advanced skills in designing, evaluating, procuring, monitoring and managing networks (SANReN, 2013a). The following section will focus on how the SANReN network is being rolled out.

### 4.4.2 SANReN Implementation

The SANReN project is being rolled out in a phased manner and will eventually connect 204 sites across South Africa to over 3 000 education and research organisations all over the world (SANReN, 2014). The beneficiary institutions mentioned in section 4.4 form the SANReN national network backbone, which is illustrated in Figure 4-3.

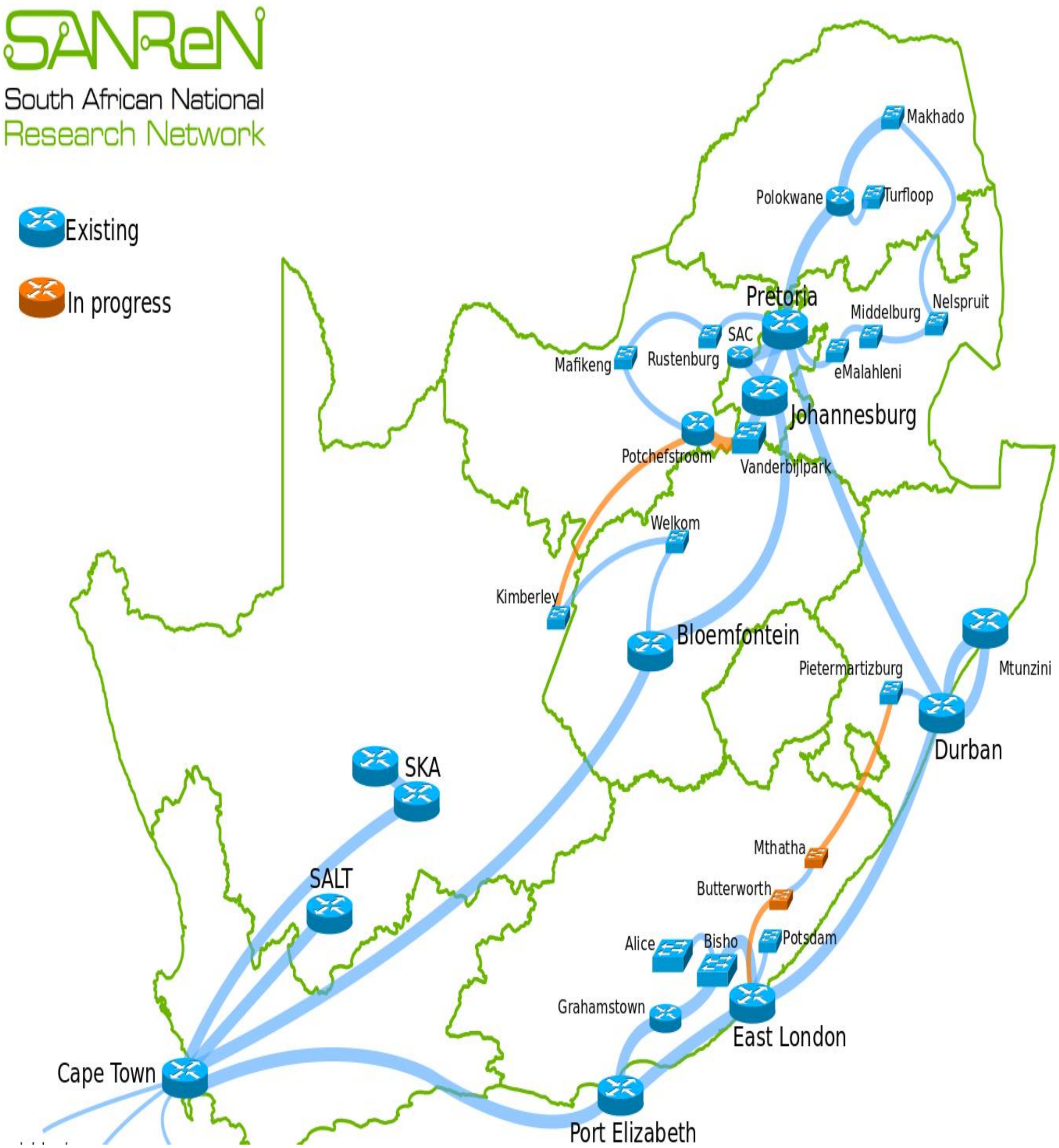

Figure 4-3: SANReN national backbone (SANReN, 2014)

The SANReN network backbone consist of 10 Gpbs 7-stretch backbone ring between the South African major cities, as depicted in Figure 4-3. SANReN Point of Presences (PoPs) are placed in all the connected institutions, namely, Pretoria, Johannesburg, Bloemfontein, Cape Town, Port Elizabeth, East London and Durban, as shown in Figure 4-3. The rolling-out of

SANReN is still progressing to other beneficiary institutions and will eventually also connect remote towns (Martin, 2012).

Figure 4-3 shows how institutions from the various provinces of South Africa are interconnected on the SANReN. The SANReN backbone network was supplied by Telkom South Africa in December 2009, with Neotel supplying the metropolitan network rings in Johannesburg and Dark Fibre Africa the optical fibre metro-ring networks in Tshwane (Pretoria), Cape Town and e-Thekwini (Durban). All these were commissioned during the years 2010 and 2011 (SANReN, 2013a). The following subsections will focus on the benefits and opportunities provided by the SANReN network.

### 4.4.3 Benefits of SANReN

SANReN has the potential to provide many opportunities and benefits to the people of South Africa. Rural areas will have increased accessibility to the Internet, which could help in addressing the digital divide (SANReN, 2012). The SANReN network is a cyber infrastructure that is attempting to close the digital divide between those who have access to the Internet and those who do not, and will connect a wide variety of people.

Currently, SANReN provides maximum accessibility and bandwidth to the educational institutions and research councils that are connected. SANReN delivers global or international connectivity with other countries, thus enabling South African researchers to be part of international collaboration that will have benefits for the country (Kuun, Wright, & Staphorst, 2013). This network also provides eduroam services to institutions and research councils and it will further expand to connect all qualifying research and tertiary institutions. The SANReN contributes immensely to the economic development of South Africa and supports huge projects of national importance such as SKA, SALT, KAT7/MeerKAT, and HartRaO/SAC for eVLBI experiments (SANReN, 2013a). The SANReN network provides many benefits to South Africa as a whole and may be regarded as one of the most important assets of the country. Therefore, it is important that the SANReN network be protected at all times in order to ensure the continued availability of the network.

### 4.4.4 Securing the SANReN Network

Many NRENs have Computer Security Incident Response Teams (CSIRTs) in place in order to respond to security incidents on the network (Moller, 2007). In this regard, the SANReN team is also in the process of establishing a SANReN/TENET CSIRT team that will be responsible for managing security incidents on the SANReN network. A CSIRT is a team of people who are responsible for receiving and responding to network security incident reports and activities (Mooi, 2013). The need for a SANReN/TENET CSIRT was identified by a survey that was conducted in May 2012 (Mooi, 2012b). This survey was sent to all the beneficiary institutions on the SANReN network with the purpose of investigating whether the beneficiary institutions would be interested in establishing a response team or a central managing party to handle incidents on the SANReN network.

Currently, the TENET NOC (Network Operations Centre) is responsible for incident handling. However, since it is the only organisation responsible for incident handling it may be hampered by restricted resources and the TENET team may lack effectiveness (Mooi, 2012b). When the SANReN/TENET CSIRT team is established, it will be responsible for protecting the SANReN network against all types of malicious activity, such as spam, denial of service attacks and hacking attempts. The responsibility of the CSIRT team will be to receive, review and respond to network security incidents (Mooi, 2012a). From a technical point of view, the SANReN network may be more secure if the SANReN/TENET CSIRT team is established; however, technical controls should not be the only concern for addressing security on the SANReN network – human factors should also be considered. In other words, the SANReN network may be vulnerable to the risks posed by human factors even if technological controls are in place.

## 4.5 Conclusion

This chapter explored the SANReN network and investigated the benefits and services that it provides to its beneficiary institutions. The SANReN is a South African NREN, while the REN of SANReN is UbuntuNet Alliance. In other words, SANReN connects to other NRENs and to the Internet through UbuntuNet Alliance. Furthermore, SANReN can be viewed as an asset or infrastructure that is critical for economic growth and an important source of technological innovation in South Africa, as it enables collaboration between South African researchers and the rest of the world. Hence, because the SANReN is viewed as a critical asset, it is important that it is protected to ensure it proper functioning in South Africa.

As stated section 1.6 (Chapter 1), technical controls alone cannot necessarily guarantee the protection of the network because these technical controls still demand and depend on human beings for implementation and maintenance. Even if technological controls do exist on the network, the SANReN network may be vulnerable to the risks posed by human factors. The following chapter will explore the human factors or human aspects in SANReN beneficiary institutions.

# CHAPTER 5: THE HUMAN FACTOR IN THE SANREN NETWORK

## 5.1 Introduction

*"Humans often represent the most important component of the information system and are chronically responsible for either the failure or the robustness of the information system. Organizations frequently seek to evaluate, select and employ a variety of controls to maintain a secure information system. In order to have the best operational information system, you must appreciate humans as the most valuable information asset*" (SANS, 2010).

The SANS institute regards the people who manage the organisation, the operating information systems and networks, and the configuring network devices, and that create the security policies of the organisation, as an organisational asset. However, because people operate, control and protect information systems and networks, they may at the same time be the cause of malfunction and failure in them. Humans have weaknesses and vulnerabilities which, if exploited, could result in severe damage to organisations' information systems and networks. These human vulnerabilities and weaknesses are the human factors that have been discussed in section 3.15.

This chapter will propose guidelines for addressing the human factors in the SANReN beneficiary institutions. The chapter will examine the human factor or human aspects in information and network security and will determine whether the human factors identified are applicable to the SANReN beneficiary institutions. The literature review will then be used to identify human factor threats. Finally, recommendations and guidelines for addressing the human factor in SANReN beneficiary institutions will be proposed.

Thus far, this dissertation has introduced the SANReN network in Chapter 1, section 1.3 and explored this in more detail in Chapter 4, section 4.4, subsequently discussing the way in which the network is being implemented, the benefits and services it offers, as well as the security of the network. The following section will give a brief review of security in the

SANReN network, as well as a brief review of the human factors as discussed in chapters 1 and 3.

## 5.2 The Human Factors in the SANReN network

As was discussed in section 3.8.1, computer networks have become assets to many organisations. Indeed, many organisations may not survive without computer networks as it may be impossible to conduct business in their absence. For this reason, as assets of organisations, the security of networks is of the utmost importance.

As mentioned in section 4.4.3, the SANReN network may be viewed as one of the most important assets of South Africa and consequently requires protection, as many research councils and universities depend on the availability of this network. SANReN has brought with it many benefits and opportunities for South African researchers; it has given South African research institutes and universities international connectivity and has enabled South African researchers to become part of international collaboration, which could assist in the economic development of the country. Therefore, the continued availability of the network must be assured and the network must be protected. Another reason for protecting the network, as mentioned in section 3.8.1, is to prevent and reduce potential network attacks and to ensure the safety of organisational operations and the people using the network.

As was discussed in section 4.4.4, SANReN is in the process of establishing a SANReN/TENET CSIRT team that will be responsible for managing security incidents on the network and increasing the level of network security. From a technical point of view, the SANReN/TENET team will ensure that security on the SANReN network will increase. However, technical controls should not be the only concern when addressing network security – the human factor is also important. As discussed in section 3.9.2, technology should not be considered in isolation from people, as it is people who are responsible for carrying out most the procedures and operations in the organisation. Hence, there will always be operational issues that are a result of human behaviour and these “human factor” issues may pose risks to the security of the network. Accordingly, if not addressed the human factor could compromise the security of the network.

Furthermore, even if technical controls such as firewalls and antivirus programs are implemented in the network (SANReN), if the human factor is neglected these technical controls will be futile. It is therefore important that, in order to provide high quality security, technical factors are considered in tandem with the human factor, because most security breaches are caused by human error. The security of networks, including the SANReN network, will always be vulnerable to human error, regardless of the technical and physical network security controls that are present. As stated in section 1.6, people are the main source of information security breaches and they are the weakest link in the security chain. Indeed, network attackers target human vulnerabilities to gain unauthorised access to systems and networks. It is therefore very important that the SANReN network address the human factor when considering the security of the network.

As mentioned in section 1.6, the human element plays a role in every network. Thus, people are involved in configuring network devices, creating security policies and participating in the network as end-users. Therefore, everyone in the organisation must have an understanding of their roles and responsibilities in order to protect the integrity, confidentiality and availability of the information in the network. For this very fact, networks like SANReN must properly address the vulnerabilities introduced by the human factor. It is thus important for end-users and IT staff at beneficiary institutions to know their roles and responsibilities and adhere to correct behaviour in order to protect the network.

The people operating the network may also be viewed as assets of the organisation, in the same way as the network is an organisational asset (SANS, 2010). However, humans (assets) in the organisation have vulnerabilities or weaknesses that have to be properly addressed because these human vulnerabilities can be exploited by various human factor threats. Because humans operate and control the information systems and networks, failure to understand the human being as an important asset that needs special attention will have a serious impact on information systems and networks (SANS, 2010).

The following section will identify some of the threats posed by the human factor in information and network security. In order to identify these threats a literature review has been conducted.

## 5.3 Identification of the Human Factor Threat in Information and Network Security

This section discusses the human factor threats that were identified through a literature review.

The following human factor threats have been identified:

- Disgruntled employees
- Terminated employees
- Human error or failure
- Insufficient security awareness
- Insufficient security training
- Insufficient security education
- Lack of security policies and procedures
- Deliberate acts of theft
- Hackers or crackers

Human factor threats are not limited to the ones listed here; however for the purposes of this research these were the ones identified as being most relevant to the study. Each of the identified human factor threats will be briefly described in the following sections.

### 5.3.1 Disgruntled employees

Disgruntled employees are angry former or current employees who may attempt to damage the facilities or equipment of the organisation as a means of seeking revenge (SANS, 2010). They purposefully or deliberately seek to damage and interrupt organisational information systems and networks (ISO/IEC 27002, 2007). Such disgruntlement could be driven by many factors, including career disappointments, retrenchment at work, dissatisfaction with the organisation or its employees, rewards inconsistent with expectations, low income and having a feeling that the "company owes me". On the basis of these factors, it is obvious that disgruntled employees could be one of the greatest threats to organisational network security of the (Holton, 2009).

As discussed in section 3.15.1, disgruntled employees could also become an insider threat (Cisco, 2008). An insider threat is an employee who uses their skills and knowledge gained through their legitimate work duties for illegitimate gain. In most cases employee disgruntlement could be the motive behind such behaviour (Robert & Siponen, 2009). Anyone in the organisation could become a disgruntled employee and could be considered an insider threat. Such disgruntled employees could be a member at the board of directors, a senior manager, a network administrator or a technical specialist (Humphreys, 2008).

### 5.3.2 Termination of Employees

Termination takes place when an employee leaves an organisation. This could be initiated by a decision of the employee or the organisation. There are two types of termination, hostile departure and friendly departure. Hostile departure is when an individual leaves a job owing to termination on various grounds, such as the organisation being taken over by new management, relocating to another location, temporary lay-offs, running out of business, forced to dismiss or fire employees or in some instances the employee simply quitting the job. With friendly departures individuals leave their jobs as a result of resignation, retirement, promotion or relocation (Whitman & Mattord, 2012). Regardless of the reason for termination, when an employee leaves an organisation there are many security-related issues to consider.

Terminated employees have the potential to cause a security breach, especially when their accounts are not disabled or when they continue to work on the day of their termination with full access rights and privileges, giving them the opportunity to create “backdoors”. During termination, employees may be tempted to steal sensitive information to sell to other companies for financial gain or might purposefully expose sensitive information or sabotage critical infrastructure, IT systems and networks out of revenge for being terminated or fired (Sarkar, 2010).

Terminating the appointment of or firing an employee could lead to employee disgruntlement, and if the termination process is not done correctly there could be serious problems. If access rights and passwords and key cards are not returned by the employee or changed, the disgruntled employee may be given the opportunity to disrupt and damage information systems and networks. When an employee is threatened with termination or during the termination process, a grief process is initiated in the employee. One of the first stages of this grief process is anger (Shaw, Post, & Ruby, 1999). Therefore, it is very important that there is a process or procedure for terminating employees in order to protect the organisation's information and network.

### 5.3.3 Human Error or Failure

Making mistakes and errors is part of being human; when people use systems mistakes are bound to happen. As mentioned in section 3.15.1, these mistakes may be caused by improper training, lack of experience, lack of supervision, lack of concentration and possible negligence. The problem with humans, according to Ashton (2009), is the limited attention and accuracy of humans, which result in mistakes, failures and errors.

As discussed in section 3.15.1, human mistakes are either accidental errors or deliberate errors. Whether accidental or deliberate, such errors could result in security vulnerabilities and, when the vulnerability is exploited, security breaches will result (Kraemer & Carayon, 2007). As mentioned in section 3.15.1, the mistakes made by employees of the organisation could threaten the confidentiality, integrity and availability of information. They could also lead to the disclosure of confidential information, entry of incorrect data or accidental deletion or modification of data, storage of data in locations that are unprotected or failure to protect information.

Employee carelessness or negligence is one of the most common and fatal causes of human error in information security and may create vulnerabilities and opportunities for criminals to steal, manipulate and corrupt information assets. For example, employees who deliberately ignore and fail to follow proper security policies and procedures, such as employees writing their passwords on sticky notes left on keyboards (Ahmed et al., 2012). Such behaviour could result in the systems and networks being unprotected. Furthermore, as mentioned in section 3.15, configuration mistakes made by careless employees could leave network ports open, firewalls vulnerable and entire systems and networks completely unprotected (Ahmed et al., 2012). Therefore, it is very important that human errors, mistakes or failure not be ignored in the organisation.

### 5.3.4 Insufficient Security Awareness

As was mentioned in section 3.16.1.1, security awareness is the start of the security learning process for all employees as it gives them an opportunity to recognise IT security concerns and security issues and to be informed on how to respond to such issues. Organisations need to promote a desire for information security in their employees; employees must know what should be protected and must be aware of the organisation's critical information assets that need protection. The purpose of security awareness is to make employees aware and interested in information security. It is intended to attract their attention and make them understand why they have to act securely (Sasse et al., 2007).

As stated in section 3.16, it is impossible to solve security problems with technology alone; thus it is important that employees are security aware and trained and educated to act as a "human firewall" in the organisation. In order for this to happen, a security education, training and awareness (SETA) programme must be in place in the organisation. The goal of such a programme would be to improve employee awareness of the need to protect system resources as well as to develop the skills and knowledge related to secure behaviour when performing their jobs.

In addition, as mentioned in section 3.16, if a SETA programme were used to create a "human firewall" this would have the potential to be more powerful than technically configured firewalls and intrusion detection systems. It can be argued that with adequate understanding, knowledge and skills, employees of the organisation could form a layer of protection similar to a firewall. Accordingly, if employees were to receive adequate security awareness training and adequate education, they might be able to identify and prevent threats to the organisation's information assets (D'Arcy, Hovav, & Galletta, 2009).

Once employees are security aware, the next level would be security training or education for certain employees with IT related roles. Employees who have participated in the awareness programme would probably respond positively to security education and further training (Sasse et al., 2007).

### 5.3.5 Insufficient security training

As was mentioned in section 3.15.3, changing the way employees behave requires breaking old habits and creating new ones through security training. While security awareness and education prepares the ground, training is what actually changes people's behaviour. In view of this, security training establishes the required behaviours in employees and should therefore be based on the work that the employee performs (Sasse et al., 2007).

As was mentioned in section 3.16.1.3, employees may play various roles in the organisation depending on their individual skills; some employees adopt the role of network administrator, while others become system administrators and so forth. Every role requires certain skills and knowledge that have to be present in order to perform the duties and responsibilities of that role. These skills can be acquired through training. Training generally is more formal than awareness programmes; it helps individuals to understand, learn about and improve their specific role, which leads to better protection of the organisation's information systems and networks overall.

### 5.3.6 Insufficient Security Education

As was mentioned in section 3.16.1.4, security education forms the advanced stage of security learning. It refers to the completion of formal education such as degrees and graduate studies in the fields of IT security and network security and may include industry-recognised IT security certification as well as programmes offered by higher education institutions. While security education can be delivered through tutorials on websites such material must provide sufficient depth of understanding in order to equip employees for dealing with the uncertainties and complexities in security decision-making (Sasse et al., 2007).

Owing to the fact that employees need to be taught about the threats that exist both outside and inside (insider threats) the organisation, social engineering methods that could be used by attackers to gain information access together with other malicious attacks such as phishing, Trojans and viruses should be emphasised. Employees should also be taught about the actions that should be taken to protect the organisation's assets (Jones & Colwill, 2008).

Time and money may be issues that influence many organisations not to provide proper security education and training for their employees. Many organisations, especially small businesses, may not be able to afford to pay for their employee education. However, regardless of whether money or time is available, all employees in the organisation should be educated about information security in line with the role they are performing (Monk et al., 2010). It is important that organisations have some form of a financial plan for security awareness education and training because if these programmes are ignored organisational assets will be left unprotected (D'Arcy et al., 2009).

### 5.3.7 Lack of Security Policies and Procedures

As mentioned in section 3.11, policies give guidance on employees' actions and behaviour by aligning behaviour with the desires of management. Policies generally direct how issues in the organisation should be addressed and how technology should be used. Procedures, on the other hand, define the technical and procedural safeguards that have been implemented to enforce specific policies; they are step-by-step instructions for implementing organisational policies.

As discussed in section 3.14, policies help by documenting the behaviour expected of employees and the consequences of violating that behaviour. Employees who do not comply with such security policies could constitute a key threat to the security of the organisation's network and related assets (Siponen et al., 2014). It is therefore important that security policies exist and are enforced in order to direct the way networks and other organisational assets are to be managed and protected.

### 5.3.8 Deliberate Acts of Theft

Theft constitutes a threat in that it involves the illegal taking of the property of another, be the property physical or electronic. Deliberate acts of theft include employees stealing computer equipment, networking devices, credentials and passwords for the purposes of monetary gain or sabotage. As was stated in section 5.3.4, human vulnerabilities may be driven by many factors such as disgruntlement, lack of accuracy and confidentiality. In the context of this study, these vulnerabilities could result in SANReN devices being stolen. For example, the IT staff at beneficiary institutions may forget to lock or secure the room in which SANReN devices are located, thus giving thieves an opportunity to steal them. Apart from having to replace the equipment, IT staff would also have to configure new devices, as well as track and correct any malicious damage.

### 5.3.9 Hackers and Crackers

Hackers and crackers are terms used for the intruders who pose a threat to organisational systems. The term “hacker” refers to a person who intentionally attempts to compromise the security of an IT system, cause disruption and obtain unauthorised access to data. The term “cracker” is a used to describe an individual who uses their advanced knowledge of networks or the Internet to compromise network security. The focal point of both hackers and crackers is people. These individuals use social engineering attacks to sidestep the technical controls of the organisation (NIST 800-16, 1998).

According to Mitnick and Simon (2002), social engineering attacks include manipulating people into performing actions or divulging confidential information. In other words, it is the exploitation of people’s natural tendency to trust individuals who seem credible (Mitnick et al., 2002). In many research studies, social engineering attacks are viewed as the most effective of all threats because they target people – who are known to be the weakest link in any organisation. A successful social engineering attack can bypass costly technical security investments to expose the organisation’s critical information and networks (Applegate, 2009). A high percentage of social attacks (hacking) are carried out by people working for the organisation (insiders), consequently a high level of threat emanates from within the organisation (Applegate, 2009).

An insider threat or an insider attack can emanate from anyone in the organisation, as long as a motive or a driving force such as revenge, anger and unfair treatment is present (Humphreys, 2008). However, insider attacks or threats can also emanate from non-disgruntled well-meaning employees, who could accidentally give malicious hackers unauthorised access to networks and systems; or could lose devices with important information which could lead to hackers compromising the security of the network (Stephens, 2010).

According to Whitman and Mattord (2012), a hacker is a classic perpetrator of espionage or trespass. Hackers and crackers are associated with deliberate acts of espionage or trespass that could result in unauthorised access to premises, systems and networks and could make networks and systems vulnerable to attacks. For example, a deliberate act of espionage or trespass could occur if a competitor (hacker) were to sneak into an organisation with a camera to record any information that could be used against the organisation.

Many organisations put a great deal of effort into protecting their assets (networks and information systems) from outside threats such as hackers and thieves, thus neglecting the inside hacker. It is therefore important that organisations understand that any of their employees could be a hacker or a cracker. Accordingly, such employees (inside hackers) may be more dangerous since they have legitimate access to and knowledge of the devices and facilities of the organisation (Padayachee, 2012). Moreover, the Internet has given hackers an opportunity to break into organisation’s system and networks without gaining physical access to the targeted systems (Kim, Jeong, Kim, & So, 2011). The following subsection will discuss the human factor threats identified in this study and Table 5-1 will show which sources were used to identify them.

### 5.3.10 Scope of the Literature Review

In order to identify the human factors involved in information and network security a thorough literature review was conducted. The aim of this review was to identify the human factors in information and network security that might be applicable to the SANReN network. The information was gathered from articles contained in information security journals, standards on international information security, books related to information security and other sources relevant to information security and network security.

Special attention was given to the following sources: information security standard ISO/IEC 27002, the SANs Institute, which was the source of most information security training content, the National Institute of Standards and Technology (800-30), which clearly lists and defines most of the threats related to human factors, as well as Whitman and Mattord’s (2012) book entitled *Principles of information security*. These sources were examined in particular to identify the threats posed by the human factor and they focus broadly on the area of information security and network security threats.

The institutions referenced are actively involved in the area of information and network security. When searching for literature on potential threats relevant to the human factor the author used the following search keywords: “threats to information security”, “threats to network security”, “threat-sources in information security”, “threat-sources in network security”, “human threats”. Literature or sources older than seventeen years were excluded for this review; however, for the rest of the dissertation they were included. These human factor threats were identified using a methodical process and are included in the list in Table 5-1.

| **Source** | **Human Factor Threats** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Disgruntled employee | Terminate d employee | Human error or failure | Insufficient security awareness | Insufficient security training | Insufficient security education | Lack of security policies and procedures | Deliberate acts of theft | Hacker or Cracker |
| (Whitman & Mattord, 2012) | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| (SANS, 2010) | ✓ | ✓ | | | ✓ | | | | ✓ |
| (NIST 800-30, 2002) | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ |
| (Huang, Rau,& Salvendy, 2010) | ✓ | | ✓ | | | | | ✓ | ✓ |
| (ISO/IEC 27002, 2007) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| (NIST 800-30, 2012) | | | ✓ | | | | | | |
| (Ahmed et al., 2012) | ✓ | | ✓ | ✓ | ✓ | | ✓ | | ✓ |
| (Kraemer, Carayon, & Clem, 2009) | | | ✓ | | ✓ | ✓ | ✓ | | |
| (NIST 800-16, 1998) | | | | ✓ | ✓ | ✓ | | | ✓ |
| (Sarkar, 2010) | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| (Lacey, 2010) | | | ✓ | ✓ | ✓ | | | | |

Table 5-1: Human factors in information security

The next section will examine the applicability of each identified human factor threat to the SANReN network. It will be argued whether the identified threats are applicable or not to SANReN. Once the human factor threats that are applicable to SANReN network have been identified, recommendations for addressing the threats will be made and guidelines proposed.

## 5.4 Applicability of identified human factor threats to SANReN

This section will argue whether or not the human factor threats identified are applicable to SANReN beneficiary institutions. The first human factor to be discussed in this regard is disgruntled employees.

### 5.4.1 Disgruntled Employees

SANReN has employed people not robots and people naturally have emotions and feelings. Therefore, people may easily become disgruntled with management or dissatisfied with the treatment they receive at work. Consequently, disgruntled employees may be viewed as a human factor threat that is applicable to the SANReN network. In this regard, both the people that SANReN network connects and the people it employs may constitute the greatest vulnerability in the security of the network. Employees working for SANReN could use the authority they have been granted to gain illegitimate access to the organisation’s information systems. As mentioned in section 5.3 disgruntled employee could be anyone in the organisation – network administrators, employees, outside contractors with insider access or end-users.

### 5.4.2 Terminated Employees

As a human factor threat, terminated employees are not applicable to the SANReN beneficiary institutions because SANReN does not employ anyone in these institutions. However, although it may be applicable to the SANReN employees in Pretoria the focus of this research is not on employees of the DST but on the people at beneficiary institutions. Since employee termination is not applicable to SANReN beneficiary institutions, step 4 as regards addressing termination of employees within the SANReN network, will not be discussed.

### 5.4.3 Human Error or Failure

This human factor threat (human error or failure) is applicable to SANReN because it is people that perform the operational duties at the SANReN and, as already established, people make mistakes. When SANReN/TENET employees are locked out of a remote configuration session (make a configuration mistake or error) with devices at beneficiary institutions, they usually ask for assistance from the IT staff at the beneficiary institutions. However, these IT staff may also make mistakes and errors while configuring the SANReN devices that could negatively affect the security of the network. Therefore, SANReN needs to consider the damage that may be caused by human mistakes and errors and must find ways of addressing this threat.

### 5.4.4 Insufficient Security Awareness

This human factor threat (insufficient security awareness) is applicable to the SANReN beneficiary institutions because SANReN does not provide security awareness training for IT staff at these institutions even though it gives them access to its network for configuration purposes. There is therefore a lack of or absence of security awareness in the beneficiary institutions, which could lead to many security risks for the SANReN network.

### 5.4.5 Insufficient security training

This human factor threat (insufficient security training) is applicable to the SANReN beneficiary institutions because SANReN does not provide security training to IT staff at the beneficiary institutions even though these people are given access to the network when making configuration changes. There is consequently insufficient security training in the beneficiary institutions that if not addressed could threaten the security of the network.

### 5.4.6 Insufficient security education

This human factor threat (insufficient security training) is applicable to the SANReN beneficiary institutions because SANReN does not provide security education to their IT staff even though these people are given access to the network in order to make configuration changes. Insufficient security education at the beneficiary institutions is thus the order of the day, and if not addressed could threaten the security of the network. As mentioned in section 3.16, uneducated employees could pose a huge risk that could put entire organisation in jeopardy.

### 5.4.7 Lack of security policies and procedures

As the SANReN network connects many communities, such as research councils, universities, schools, hospitals and government departments, policies should be in place to govern network usage. This human factor threat (lack of security policies and procedures) in SANReN beneficiary institutions is applicable to SANReN because, according to an interview that was conducted with the SANReN network engineer, although SANReN does have security policies place these might nevertheless be insufficient in addressing the human factors in the SANReN network. Furthermore, no defined roles, responsibilities or operational procedures for the management of the SANReN devices have been identified at the beneficiary institutions.

### 5.4.8 Deliberate acts of theft

This human factor threat (deliberate acts of theft) is applicable to the SANReN beneficiary network because theft of SANReN devices at beneficiary institutions could occur if there are no specific measures or procedures in place for the use of these devices.

### 5.4.9 Hackers and crackers

This threat (hackers and crackers) is applicable to SANReN owing to the fact that, despite the nature of the organisation, there may be people who would like to see the network fail. These people could exist both inside and outside the beneficiary institutions. Those outside these institutions may attempt to exploit the vulnerabilities or weaknesses of people who have access to the network, while those inside (IT staff at beneficiary institutions) could use their legitimate access to cause harm or damage to the network

The next section will discuss ways of addressing the human factor threats that are applicable to the SANReN network. On the basis of the literature studied, it will determine how these human factors are generally addressed and will discuss the way SANReN is currently addressing them. Apart from terminated employees, which will not be discussed in the following section, it has been found that disgruntled employees, human error or failure, insufficient security awareness, insufficient security training, insufficient security education, lack of security policies and procedures, deliberate acts of theft, and hackers and crackers are all applicable to SANReN beneficiary institutions.

## 5.5 Addressing human factor threats in SANReN

This section will examine how each of the human factors that have been identified as being applicable to the SANReN is generally addressed according to the literature. It will also determine whether or not SANReN is currently addressing them. Subsequently, recommendations and guidelines for addressing the applicable human factor threat within the SANReN beneficiary institutions will be provided. The following three questions will be asked with regard to all the human factor threats that are applicable to SANReN:

a. **How are the human factor threats addressed in general?** (This section will discuss ways of addressing the identified human factor threats.)

b. **Does SANReN currently address the human factor threats related to the beneficiary network?** (This section will determine whether the SANReN is currently addressing the human factor threats and the measures it has taken to address them.)

c. **What are the recommendations for addressing the human factor threats in SANReN beneficiary networks?** (This section will discuss and recommend ways of dealing with the identified human factor threats. Guidelines for addressing the human factor in the SANReN will be proposed.)

### 5.5.1 Disgruntled Employees

#### 5.5.1a Addressing Disgruntled Employees

Addressing a disgruntled employee is not an easy task, as there may be many factors prompting the employee's anger and which may be difficult to address. In order for organisations to address the threat this poses, they need to foster a security aware culture or information security culture. As discussed in section 3.15.3, this type of culture will shape the way in which employees should conduct themselves when protecting the information assets of the organisation. It may also help to bring about changes in the way employees behave with regard to security, to make them more security aware and to encourage them to follow good security practices when performing their everyday activities (Cisco, 2008; Colwill, 2009).

In addition to the development of an information security culture, an organisational culture should be developed to address this human factor threat. As was mentioned in section 3.14, organisational culture includes the attitudes, values, beliefs, norms and customs of the organisation and it develops as a result of employee behaviour. It is therefore important to consider the organisational culture when fostering an information security culture so as to ensure that the most appropriate controls are identified and successfully deployed (Veiga & Eloff, 2010). It is very important for organisations to have a balanced organisational culture as it establishes the way employees should behave in the organisation (Thomson et al., 2006).

An effective organisational and information security culture will make it difficult for a disgruntled employee to do harm or disrupt IT systems and networks. For employees to be happy in their work and in the organisation they work for they need to feel part of a team that cares, and they need to feel safe, secure and appreciated. If that type of culture does not exist and employees believe that the organisation does not care about them, they could become disgruntled. Such a disgruntled employee now becomes an insider threat or could provide a perfect target for other threats (Humphreys, 2008).

The following section will discuss the current measures in place at the SANReN beneficiary institutions in order to addresses the threat of disgruntled employees. In other words, it will discuss what SANReN is currently doing to deal with this threat.

### 5.5.1b Is SANReN currently addressing the threat of Disgruntled Employees in the Beneficiary Institutions?

SANReN does not need to address the human factor threat of disgruntled employees as it has no employees at the beneficiary institutions. Instead SANReN/TENET uses remote access to make configuration changes on its networking devices at beneficiary institutions. As was stated in section 4.1.1, TENET has about 12 full-time staff in Cape Town and Johannesburg, while SANReN has about 15 full-time staff in Pretoria. Although there are no SANReN/TENET employees working at the beneficiary institutions, when the remote access to the devices at beneficiary institutions fail, IT staff at these institutions are granted access in order to make configuration changes.

In other words, although there are no people working for SANReN at the beneficiary institutions, SANReN/TENET makes use of the institutions' IT staff when they need to install or configure networking devices. Because the focus of this research is on the human factor in the beneficiary institutions of the SANReN network and not the SANReN/TENET employees in main offices (Pretoria, Cape Town and Johannesburg), it was found that SANReN does not address the threat of disgruntled employees at beneficiary institutions. The reason for this is that SANReN does not regard itself as having employees at these institutions even though the IT staff may be viewed as employees of SANReN since they are sometimes granted access to the network.

### 5.5.1c Recommendations for addressing Disgruntled Employees within the SANReN Beneficiary Institutions

The IT staff at the SANReN beneficiary institutions could become angry with SANReN/TENET because although it does not employ them, when it is experiencing problems with the network these employees are required to stop their own work and focus on the SANReN/TENET network. In addition, the lack of appreciation or reward for the work done could also lead to IT staff feeling disgruntled.

When someone knows that they are not accountable for something they will probably not perform with the same level of accuracy, concentration or dedication. Humans have vulnerabilities and these vulnerabilities can be driven by many factors such as anger (disgruntled). For example, the IT staff at beneficiary institutions may forget to lock or properly secure the room where these networking devices are located, thus creating an opportunity for equipment to be stolen, which will then have to be replaced by the beneficiary institution. Subsequently, IT staff will also have to configure the new device and track and correct any malicious damage. This will result in the productivity, time and money that could have been used for other business functions being wasted because of the human factor (disgruntled employee).

Furthermore, stolen equipment may contain critical data that could be used for malicious purposes and may be difficult to replace. SANReN consequently needs to think about all the human factor related threats that may place the security of the network at risk. It is therefore, recommended that SANReN/TENET should employ people at the beneficiary institutions that will work specifically for SANReN. Such people would them be dedicated to the security of the network and would perform all the configurations to the networking device while residing at the beneficiary institutions. Therefore, the first guideline proposed by this dissertation is that:

**SANReN/TENET management should employ people at SANReN beneficiary institutions to work specifically for SANReN/TENET**.

When it comes to SANReN employing people at the beneficiary institutions finances could be an issue. However, the security of the SANReN network should be the priority; therefore, it is important to view this recommendation from a security point of view. For example, will it benefit the SANReN network if SANReN/TENET is only willing to invest in the provision of technology and not the operational side (people) as well? Even, the same technology provided would still demand and depend on people for implementation and maintenance. Investing in people is part of investing in operational security, and this may add another layer of security to the network. Many researchers agree that the use of technology alone will not ensure the safety of systems and networks; people (operational) also need to be invested in, to be considered and to be given more attention (Furnell & Clarke, 2012; Van Niekerk & Von Solms, 2010; Ashenden, 2008; Kraemer & Carayon, 2007; Thomson & Von Solms, 2006). The foundation of good security is the people involved; hence, investing in people is investing in the security of the SANReN network.

As it is clear that there are no measures in place at SANReN beneficiary institutions that specifically deal with the disgruntlement of employees, the following guideline is proposed by this dissertation to address it:

**SANReN/TENET should develop an information security culture to shape and influence the behaviour of IT staff at beneficiary institutions**.

Only once people employed by SANReN are working at the beneficiary institutions (as proposed by the first guideline) will an information security culture (i.e. the second proposed guideline) develop at these institutions. It is important to understand that what is proposed by the first two guidelines could take a long time to be established because of a lack of resources such as finances. However, the other guidelines could be easily implemented in a short period of time compare to the first two guidelines proposed above.

The following section will provide recommendations and guidelines for addressing the threat of human error or failure in SANReN beneficiary institutions.

### 5.5.2 Human Error or Failure

#### 5.5.2a Addressing Human Error or Failure

Adequate security education, training and awareness must exist in the organisation in order to address and prevent human errors, mistakes or failures from threatening the security of the network. All employees, contractors and third parties must have an adequate level of awareness, education and training in security procedures and the correct use of information processing facilities (ISO/IEC 27002, 2007). As mentioned in section 3.15.4, this security training, awareness and education should be provided in line with the employee's job function in order to reduce the security risks that could be posed by human error.

As already mentioned in section 3.15.1, human error or failure with regard to the security of the network can be prevented or addressed with security training, continuous awareness-raising activities and controls. Controls include procedures such as the verification of commands by a second party or forcing the user to type critical commands twice. Security awareness education should form part of every employee's job thus keeping security at the forefront of every employee's mind to reduce mistakes and errors.

According to the international standard ISO/IEC (2007), a formal information security event reporting procedure should be in place, together with an incident response and escalation procedure, stating the action to be taken on receipt of a report of an information security incident. Furthermore, it is important that there is a point of contact for reporting information security events. This point of contact should be known throughout the organisation, should always be available and should be able to provide adequate and timely response (ISO/IEC 27002, 2007). In addition, in order to address human error and mistakes in organisations, employees must be aware of information security threats and concerns and their roles, responsibilities and liabilities in this regard, and they must also be equipped to support the organisational security policy when performing their normal work.

### 5.2.2b Does SANReN currently address the threat of Human Error or Failure within the Beneficiary Institutions?

Currently SANReN does not address the threat of human error or failure in the beneficiary institutions even though there is the potential for IT staff to make errors and mistakes when configuring SANReN devices. Moreover, no provision has been made for security education, training and awareness for the people at the beneficiary institutions.

### 5.2.2c Recommendations for addressing Human Error or Failure within the SANReN Beneficiary Institutions

Human error or failure may affect the integrity, confidentiality and availability of many if not all critical systems on the network. Just as technical failures and mistakes can be avoided through proper technical training, human failures and mistakes can be avoided through a proper awareness programme and proper training.

Security education, training and awareness (SETA) should be used to create a proper understanding of the consequences that human mistakes and errors have for the security of the SANReN network. According to Cisco (2008), all employees should receive security education and training in order to understand what they have to do to protect the network and information systems, why they should act securely and how they must behave (Cisco, 2008). Because IT staff at the SANReN beneficiary institutions interact with the network, it is recommended that SANReN/TENET should establish a security education, training and awareness (SETA) programme in order to address human factors such as human error and failure in the SANReN network.

Furthermore, security workshops should be held and presentations made regarding the security of the SANReN network with the purpose of educating IT staff at beneficiary institutions on how to behave while using the SANReN devices. These security presentations and workshops should include demonstrations and examples of human error, and should demonstrate how those errors could compromise the security of the SANReN network. Therefore, the second guideline proposed by this dissertation is:

**SANReN/TENET should establish a security education, training and awareness (SETA) programme for beneficiary institutions in order to address human factors such as human error or failure in the SANReN network.**

The next section will discuss the threat posed to SANReN beneficiary institutions by insufficient security awareness. This discussion will follow the three steps listed in section 5.6 and will start by discussing how the threat is addressed according to the literature. It will then move on to discuss the way SANReN is currently addressing the threat and then make recommendations and propose a guideline to counter the threat.

### 5.5.3 Insufficient Security Awareness

#### 5.5.3a Addressing Insufficient Security Awareness

According to the international standard ISO/IEC (2012), employees should be required to undergo a minimum number of hours of awareness training in order to ensure that they are aware of their roles and responsibilities when using both cyberspace and the organisation's systems and networks. The awareness training should include content such as (ISO/IEC 27032, 2012):

- Information on the latest threats and the various types of social engineering attacks, for example how phishing has evolved from fake websites alone to a combination of spam, cross site scripting, and SQL injection attacks.
- Information on the way both individual and organisational information could be stolen and manipulated through social engineering attacks and how attackers can take advantage of human nature; for instance the tendency for humans to comply with requests that are made with authority which results in people being victims of social engineering attacks.
- The type of information that needs to be protected and how this should be done in accordance with the information security policy

When employees are aware of security-related breaches, it is easier for them to detect and report possible malicious activities (Jones & Colwill, 2008). Additionally, once awareness training programmes have been conducted, an organisation could conduct periodic tests in order to determine whether employees have understood what they were taught and also to determine whether employees comply with the security policies and practices of the organisation (ISO/IEC 27032, 2012).

The National Institute of Standards and Technology (NIST) recommends the following in addressing security awareness (NIST, 2007):

- Implement a formally documented security awareness and training policy.
- Provide basic security awareness training for all users of information systems in the organisation.
- Provide specific information system security training to individuals identified as having significant information system security roles and responsibilities within the organisation.
- Document, monitor and record security awareness and information system security training for all personnel in the organisation to ensure compliance and refresher training as dictated by company policy.

### 5.5.3b Does SANReN currently address Insufficient Security Awareness within the Beneficiary Institutions?

As mentioned in section 5.6.2, SANReN currently has no security awareness programme in place at the beneficiary institutions and, thus, the resulting lack of security awareness could threaten the security of the network.

### 5.5.3c Recommendations for addressing Insufficient Security Awareness within the SANReN Beneficiary Institutions

It can be argued that the SANReN/TENET has assumed that the IT staff at the beneficiary institutions are capable of secure behaviour and that they have all the knowledge, skills and understanding required for perform every task given to them. However, according to Monk et al., 2010), it can never be assumed that an individual is capable of behaving securely. It is therefore important to ensure that adequate knowledge and skills are transferred to the individual through security awareness, training and education.

Every individual who is to work with the organisation’s systems and networks should first undergo security awareness training before being given access. However, with the SANReN network the IT staff at beneficiary institutions, who are often asked by SANReN/TENET to make configuration changes, have not undergone any security awareness training before being granted access to the network, thus exposing the network to a variety of human errors and mistakes that could threaten it. It is therefore recommended that the SANReN network should establish an appropriate security awareness training programme for all beneficiary institutions, specifically focusing on the IT staff that may be allocated to help SANReN/TENET with operational duties.

According to the international standard (2012), employees are the main entry point for social engineering attacks; therefore, they need to be aware of security-related risks. It is the responsibility of the organisation to encourage its employees to learn about and understand security-related risks (social engineering risk) and the steps they must follow to protect both themselves and the organisation against potential attacks (ISO/IEC 27032, 2012). Therefore the guideline proposed by this dissertation to address the threat of insufficient security awareness is:

**All SANReN beneficiary institutions should implement security awareness program that includes focus on issues relating to securing the SANReN network.**

The following section will discuss the threat of insufficient security training that is applicable to the SANReN beneficiary institutions. As in the previous sections it will follow the three steps listed in section 5.6.

## 5.5.4 Insufficient Security Training

### 5.5.4a Addressing Insufficient Security Training

In addressing the threat of insufficient security training for employees, the International Organization for Standardization (2012) states that employees in the organisation should be adequately trained in order to develop the required skills and expertise. Furthermore, they should be trained to respond effectively and efficiently to specific security threats. For employees to be adequately trained the following must exist (ISO/IEC 27032, 2012):

- Focused training sessions, with simulated cyber-attack scenarios and workshops on specific areas of required action should be designed, organised and delivered. These focused training sessions and workshops should be offered to employees on a regular basis, and must include updates.
- Regular testing with walkthroughs of relevant scenarios to ensure a comprehensive understanding and ability to execute procedures and use specific tools.

- Regular briefings on cyber security risk status and findings concerning the organisation and the industry should be provided.

As was stated in section 3.10, network security professionals should attend training and workshops on security threats and have access to new security tools, protocols, techniques and technologies. Both internal and external experts can provide security training (as well as awareness and education). It is important that employees are provided with hands-on security training in order to improve their skills and confidence in behaving securely (Siponen et al., 2014). Scenarios must be used as part of the training process as these will enable individuals to gain real-life experience of relevant situations, and to learn and practise the responses required. Furthermore, past incidents could be used as part of the scenarios to learn and gain more understanding.

### 5.5.4b Does SANReN currently address the Threat of Insufficient Security Training within the Beneficiary Institutions?

As with security awareness, SANReN/TENET is currently doing nothing in SANReN beneficiary institutions to provide security training. As was mentioned in section 5.6.3, SANReN currently has no security training programme in place at the beneficiary institutions and, as a result, employees may be inadequately trained in that regard which could result in human error in the network.

### 5.5.4c Recommendations for addressing Insufficient Security Training within the SANReN Beneficiary Institutions

SANReN connects different institutions in South Africa and some of these are situated in disadvantaged areas that might lack highly trained IT professionals. What if a low-skilled individual were asked to perform the configuration changes on the SANReN network devices? This could result in devices being misconfigured, consequently creating more problems on the network. For example the employee could, having been granted access to the networking devices, knowingly or unknowingly connecting a device which contains viruses and worms, which may then be distributed throughout the network and which could have a severe impact on network security. By allowing IT staff at the beneficiary institutions access to the network, SANReN could be granting access to an insider threat.

As was mentioned in section 5.3.4, humans have vulnerabilities and these vulnerabilities may be driven by many factors such as lack of security training, limited attention, anger, carelessness or even curiosity. Some people may be driven by curiosity to configure incorrect commands such as “I just want to know what will happen to the network if configure this …” Some IT staff at the beneficiary institutions may even be driven by anger, as discussed in section 5.3.4, in response to doing tasks or a job that has no compensation or when he or she has to stop doing their own job to focus on something that is not really their responsibility.

It is therefore recommended that the SANReN/TENET should implement a security training programme for the beneficiary institution to equip IT staff with the skills needed when given access to SANReN networking devices. The programme should cater specifically for those who generally help SANReN/TENET when it needs assistance. These programmes should be both ongoing and once-off, as new threats arise daily to attack the network. The guideline proposed for addressing this threat in SANReN beneficiary institutions is:

**SANReN/TENET should implement a security training programme for beneficiary institutions in order to provide appropriate skills and knowledge for ensuring that the interface connecting to the SANReN network from the beneficiary institution is protected.**

The following section will discuss the threat of insufficient security education that is applicable to SANReN beneficiary institutions. It will follow the three steps listed in section 5.6, as was done in the preceding sections.

### 5.5.5 Insufficient Security Education

#### 5.5.5a Addressing Insufficient Security Education

To address the threat of insufficient security education for employees and minimise possible security risks, the organisation should provide adequate training on security procedures and the correct use of information processing facilities. Security education (as well as awareness and training) should be suitably designed and relevant to the employee’s role, responsibilities and skills and should also include information on known threats, whom to contact for further security advice and the proper channels for reporting information security incidents (ISO/IEC 27002, 2007).

Additionally, a formal disciplinary process for employees who have committed a security breach should be implemented. This process should take into consideration the severity of the breach and the impact it has had on the organisation. Disciplinary measures that could result may be instant termination of employee, or the removal of access rights and privileges (ISO/IEC 27002, 2007). If employees are properly educated and trained and are aware of security risks, cases of misconduct leading to disciplinary actions will decrease.

Further, motivation with regard to information security may increase if the organisation were to develop an internal security certification programme which gives employees company security certification after completing it. These certificates could be similar to the ones the IT professionals receive after completing a certain course or training. Such certification could recognise and motivate non-IT employees who are actively involved in helping to secure the information of the organisation. In addition, a reward programme could be instituted to get employee motivated with regard to security education, training and awareness. For example, if no security incident occurs, such as no virus infections for a certain period in the network, all employees get an extra day of leave the following year. This would show management commitment and support for security and employees would start to change their attitude and behaviour towards security (Hight, 2005).

### 5.5.5b Does SANReN currently address the Threat of Insufficient Security Education within the Beneficiary Institutions?

Like security awareness and training, SANReN/TENET is currently not doing anything in its beneficiary institutions to provide employees with security education; as a result human errors in the network could leave it vulnerable. SANReN/TENET is currently assuming that the people at the beneficiary institutions have all the qualifications, knowledge and skills required without actually investigating whether this is indeed so or providing them with the training they need. Just because an individual claims to have a certain qualification does not mean that he or she can perform the job correctly or that the qualification actually exists. Even the most trusted employees may have false qualifications; they may claim to have degrees or qualifications that they do not.

For example, recently in South Africa it was discovered that “Dr” Pallo Jordan, a former minister of arts and culture, senior member of the African National Congress (ANC), current member of the parliament and a representative to the Pan-African Parliament did not have the academic qualifications he claimed to have. According to *Times LIVE* reporter Van Onselen (2014), Mr Jordan had no degrees or diplomas from the University of Wisconsin-Madison or the London School of Economics (LSE), which he had claimed to have obtained. Furthermore, Mr Jordan had never had an honorary doctorate presented to him and had no formal tertiary academic qualification of any kind.

If someone of that calibre is able to keep such information under wraps for such a long time, what would stop the IT staff at the beneficiary institutions? It is the responsibility of SANReN/TENET to ensure that the people who interact with their network are adequately educated. Anything could go wrong while configuring the network devices especially if the people configuring them are unqualified and lack the skills needed to perform the job. It is important to perform a background check on individuals, especially as regards their qualifications, before they are given access to the network.

#### 5.5.5c Recommendations for addressing Insufficient Security Education within the SANReN Beneficiary Institutions

There is a need to educate and persuade the employees of the organisation (whether they are IT professionals or not) to think and act in a security conscious way. As was mentioned in section 3.15.4, the purpose of security education, training and awareness is to create a proper understanding of the threats facing information systems and how people should behave in response to those threats.

It is therefore recommended that the SANReN/TENET should provide an adequate level of security education to the SANReN beneficiary institutions in order to ensure that the people that they are allowing to access their networks are knowledgeable, sufficiently skilled and qualified to interact with the network. Establishing a security education programme for the beneficiary institutions could also improve the level of trust between them and SANReN and would also decrease the potential for disgruntled employees. Security education together with training and awareness programmes could also help to promote an understanding of both the security policies and the controls that are applied (Jones & Colwill, 2008).

As mentioned in section 3.16.1, security education is a continuous process; it starts with the awareness stage, moves on to training and then to education. It is therefore very important that the people at the beneficiary institutions go through those learning processes in order to adequately protect the SANReN network. As was mentioned in section 3.10, security education, training and awareness forms the strongest defence against network breaches; therefore SANReN needs to establish a SETA programme for the beneficiary institutions specifically targeting their IT staff.

Security education, training and awareness forms the steps taken to change people's behaviour towards security. It is important that, once security awareness, education and training have been effectively implemented in the organisation, employees are given regular reminders of the key messages. Such reminders could include posters, trinkets and screen savers with security messages to remind the employees about security. However, these reminders must not replace the regular awareness education and training programmes (Sasse et al., 2007; Jones & Colwill, 2008). Accordingly, the guideline proposed for addressing this threat in SANReN beneficiary institutions is:

**SANReN/TENET should ensure that the IT staff at beneficiary institutions have appropriate qualifications, training, experience and certification before granting them access to SANReN devices.**

The following section will discuss the threat posed by a lack of security policies and procedures in SANReN beneficiary institutions. As before, it will follow the three steps listed in section 5.6.

## 5.5.6 Lack of Security Policies and Procedures

### 5.5.6a Addressing the Lack of Security Policies and Procedures

In addressing the lack of security policies and procedures, management should publish an information security policy which should be communicated to all employees and relevant external parties of the organisation. This information security policy must include the security roles and responsibilities of every employee in the organisation. These security roles and responsibilities should include the requirement to (ISO/IEC 27002, 2007):

- implement and act in accordance with the organisation's information security policies
- protect assets from unauthorised access, disclosure, modification, destruction or interference
- execute particular security processes or activities
- ensure responsibility is assigned to the individual for actions taken
- report actual or potential security events and other security risks to the organisation.

The allocation of information security roles and responsibilities should be done in accordance with the information security policy. Employees with allocated security responsibilities may delegate the security tasks to other employees but they still remain responsible for the task and will need to ensure that it is done correctly (ISO/IEC 27002, 2007).

Information and networks could be compromised by a lack of security policies or procedures. For example, it is important that an access control policy be established, documented and reviewed periodically in the organisation in order to control access to critical assets. Such an access policy should clearly state the rules and rights for each employee or user and should be supported by formal procedures with clearly defined responsibilities. The granting of access rights to users or employees should be on a need-to-use and an event-by-event basis in line with the access control policy. It also important that formal procedures are in place to control the granting of access rights to information systems and services. Accordingly, operational procedures must be documented, maintained and made available to all employees who need them. In addition, the roles, responsibilities and procedures for the management of remote equipment, including equipment in user areas, should be established and defined (ISO/IEC 27002, 2007).

### 5.5.6b Does SANReN currently address the Lack of Security Policies and Procedures in Beneficiary Institutions?

An investigation into the existing policies that oversee the use of the SANReN network was conducted. The authors consulted network engineers from SANReN concerning the current policies between SANReN and the SANReN beneficiary institutions. The authors were then directed to the TENET website where the policies relating to SANReN and the beneficiary institutions were located. In these policies the authors were specifically looking for the operational roles and responsibilities of people in the SANReN network. The following questions were asked to focus the content analysis of these policies:

- Who is allowed to have physical access to the SANReN devices of the beneficiary institutions?
- Who can configure SANReN devices in the beneficiary institutions?
- What minimum skills or qualifications should the people who configure SANReN devices in the beneficiary institutions have?
- Are there training programmes or some other form of education available at the beneficiary institutions connected to the SANReN network?

The following policies were examined in order to determine whether the human-related issues regarding the previous questions have been addressed in the TENET policies. These policies were the only ones on the website and according to the people at SANReN these are the only ones that currently govern the use of the SANReN network. They include the Acceptable Use Policy (AUP), the Connection Policy and the Privacy Policy. These policies were all created by TENET, because it is the operating entity for the SANReN network. These policies are to the authors' knowledge the only ones that manage the use of the SANReN network. An analysis of these three policies was done in order to identify whether human factors are addressed in the policies. This will be discussed in the following subsections.

### Acceptable Use Policy (AUP)

The purpose of the TENET AUP is to outline the things that are allowed and disallowed on the network in the SANReN beneficiary institutions. The policy outlines the rules and responsibilities of SANReN beneficiaries and participating institutions. According to the TENET AUP, beneficiary institutions are allowed to use the REN services for any legal activity that furthers the goals and aims of the institution only if such activity does not include any unacceptable uses. If the beneficiary institution does anything unacceptable on the network, the policy states that TENET may discontinue REN services.

A few of the unacceptable uses of REN services that are listed in the TENET AUP are:

> Any attempt to use the REN services in a way that breaches or would breach the security of another user's account or those gains or would gain access to any other

person’s computer, software, or data or otherwise threaten another person’s privacy, without the knowledge and consent of such person.

Any failure to secure a server that is connected via the REN services to the Internet against being abused by third parties as an open relay or open proxy.

Any effort to use the REN services in a way that circumvents or would circumvent the user authentication or security of any host, network account (“cracking or hacking”).

With regard to the questions posed previously, the TENET AUP has nothing to say about physical access to SANReN devices at beneficiary institutions, nor about who is allowed to configure SANReN devices. Moreover, nothing is said about the level of skills or qualifications of people configuring SANReN devices at beneficiary institutions or about any form of training programme for beneficiary institutions.

**Connection Policy**

The Connection Policy lists all the types of connection that are available when connecting an REN. This policy specifies the differences between the connections and the rules and responsibilities attached to each. The types of REN network connection include direct on-site connection, direct PoP connection and indirect connection. The direct on-site connection is a connection type that is under TENET operational management where the hand-off location is at the connecting site, not the connecting party (beneficiary institutions). Hand-off location is the point where operational responsibility changes between the beneficiary institution and TENET (TENET, 2014).

For the direct PoP connection the hand-off location is at the Point of Presence and TENET does not operate the terminating equipment at the connecting site nor does it operate the access circuit between the connecting site and PoP. The institutions that have direct connection can then provide an indirect connection to other smaller research and education organisations around them. In this way, institutions such as education and training colleges, schools and public museums can connect to the beneficiary institution’s direct connection in order to access the REN services. However, the indirect connection is the responsibility of the SANReN beneficiary institution – not TENET. With regard to the questions previously posed, the TENET Connection Policy does not mention anything about physical access to SANReN devices in beneficiary institutions nor the configuring devices. Also nothing is stated about the level of skill or the qualifications required by the people configuring SANReN devices at the beneficiary institutions and nothing is mentioned about a training programme for beneficiary institutions provided by SANReN/TENET.

### Privacy Policy

The TENET Privacy Policy explains how the personal information that TENET collects from its contacts is used. TENET contacts are the people who work with it such as representatives of the beneficiary institutions, suppliers and other contractors (TENET, 2014). The TENET Privacy Policy states that TENET respects the privacy of its contacts and will protect the confidentiality of their personal information. With regard to the questions previously posed, the TENET Privacy Policy does not say anything about physical access to SANReN devices in beneficiary institutions or about the people who are allowed to configure these devices. Moreover, nothing is stated about the level of skills or qualifications required by people configuring SANReN devices at the beneficiary institutions or about any form of training programme which may be provided to the beneficiary institutions by SANReN/TENET.

After conducting an analysis of the TENET policies, it can be noted that the AUP, the Connection Policy and the Privacy Policy do not adequately address the human factors that might pose risks to the security of the SANReN network, as none of the policies state the operational roles, responsibilities and procedures on the SANReN network. There was no documented framework for dealing with the security vulnerabilities posed by the human factors on the SANReN beneficiary network and no clear guidelines or procedures concerning things like access control and authorisation.

In addition, nothing was mentioned about accessing the network devices or about locking the doors or monitoring the rooms where these devices are placed. In other words, no direct rules and responsibilities or operational procedures are addressed in these policies. Consequently, if there are no proper procedures in place the security of the network may be at risk and it may be easier for unauthorised individuals to gain access to the devices and, intentionally or unintentionally, misconfigure them. Once an unauthorised person has gained access to the devices even the technical solutions will not help in protecting the network.

### 5.5.6c Recommendations for addressing the Lack of Security Policies and Procedures in the SANReN Beneficiary Institutions

Policies are like laws – they define what is right and wrong and state the penalties for violation. They are one of the key ways in which humans interact with security mechanisms and it is in the interpretation of these policies that human vulnerabilities often occur (Sasse et al., 2007).

It is therefore recommended that a security policy addressing operational concerns, namely, an operational security policy, be put in place in the SANReN network and be enforced in all the beneficiary institutions. Policies that outline the responsibilities and roles of people in the beneficiary institutions should be in place to better secure and manage the SANReN network. Access control policies regarding the SANReN devices at beneficiary institutions should be established, documented and reviewed by SANReN in order to control access to devices. Such policies should be implemented in the beneficiary institutions and should explicitly state who has access to SANReN devices, the level of access the individual has and whether the individual is allowed to make configuration changes.

Formal procedures need to be in place to control the operation of devices and control the granting of access rights to the SANReN network. There should be clear specifications for the roles and responsibilities of IT staff at beneficiary institutions and operational procedures should be documented and maintained, and subsequently made available to all IT staff.

Therefore the guideline proposed for addressing this threat in SANReN beneficiary institutions is:

**SANReN/TENET should develop security policies that address operational concerns relating to the interface between the SANReN network and the beneficiary institution.**

The following section will discuss the threat of deliberate acts of theft in SANReN beneficiary institutions. In doing so, it will follow the three steps listed in section 5.6, as done previously.

### 5.5.7 Deliberate Acts of Theft

#### 5.5.7a Addressing Deliberate Acts of Theft

In addressing acts of theft a wide variety of measures can be implemented, including locked doors. To this end, access control policies should be implemented to protect equipment from theft (Whitman & Mattord, 2012). Persons with access to networking equipment or devices should be clearly specified (who can access what and who has the key to the room where devices are located). The security of the physical location where networking devices and equipment are placed and the securing of the actual device are very important because a breach of physical security can result in a loss of information. Physical security can include locks and keys and these should be used to restrict access to and interaction with the equipment. Furthermore, security personnel should be properly trained and should always be vigilant in protecting the organisational assets (Whitman & Mattord, 2012).

#### 5.5.7b Does SANReN address Deliberate Acts of Theft in the Beneficiary Institutions?

In the SANReN beneficiary institutions the threat of deliberate acts of theft is not adequately addressed. There are no access control policies specifying who is allowed or not allowed in the room where the equipment is situated. If all the IT staff at beneficiary institutions have access to this equipment problems may be experienced because there may be disgruntled employees who intentionally leave the doors unattended for outsiders (hackers) to illegally gain access to the SANReN network.

#### 5.5.7c Recommendations for addressing Deliberate Acts of Theft in the SANReN Beneficiary Institutions

Physical security measures, such as doors with access control systems (access control policies), should be in place where networking devices and equipment are located at beneficiary institutions. Monitoring systems such as CCTV should also be used in combination with other controls in order to protect the assets of the organisation. Even if a disgruntled employee knows that all these controls and other effective security measures are in place in the organisation such measures will make it more difficult for him or her to carry out malicious acts because there is good chance of being caught. When an employee leaves the organisation, a carefully managed termination process should be in place to prevent possible information or equipment theft. It is recommended that procedures, which include the roles and responsibilities (operational duties) of people at SANReN beneficiary institutions, should be clearly defined. Therefore the guideline proposed by this dissertation for this threat is:

**SANReN/TENET should establish formal operational procedures specifying the roles and responsibilities of IT staff at beneficiary institutions**

The following section will discuss the threat posed by hackers and crackers in the SANReN beneficiary institutions. It will follow the three steps listed in section 5.6.

### 5.5.8 Hackers and Crackers

#### 5.5.8a How to address Hackers and Crackers

Hackers rely heavily on social engineering attacks to circumvent technical controls. Consequently, measures to address hackers and crackers go hand in hand with those to address social engineering attacks (Applegate, 2009).

The most effective way of addressing hackers and crackers is to develop defences that use multiple techniques. Such techniques should include education, which is regarded as the best way to address this threat. The more employees understand this type of threat, as well as the techniques or methods used to carry out such an attack, the more likely they will be to resist and report it. Security awareness training and security policies should be developed to protect the organisation's systems and networks against this threat (Applegate, 2009).

#### 5.5.8b Does SANReN currently address Hackers in the Beneficiary Institutions?

At the SANReN beneficiary institutions human factor threats such as hacking have not been addressed because no security education or awareness training is in place at the beneficiary institutions.

### 5.5.8c Recommendations for addressing Hackers in the SANReN Beneficiary Institutions

Attackers or hackers are no longer targeting machines to gain access to networks and information systems; they now target the people who operate these machines. Attackers have matured; from using hacking skills just for fun of it or to show off their technical skills, they now use these skills for financial gain and to disrupt systems (Dlamini, Eloff, & Eloff, 2009).

An outside hacker could go to the beneficiary institutions and pretend to be someone from SANReN/TENET. Consequently, because of people's tendency to comply with requests that are made with authority and to be helpful, the IT staff at beneficiary institutions may very well grant this individual access to the SANReN networking devices. The attacker would then have access to the network and so what they like, such as intentionally infect the network with viruses or worms. This could have a disastrous effect on the entire network and could ultimately result in a fatal network failure.

Therefore SANReN/TENET should certainly address this human factor threat, and security education and awareness training should be provided for people at the beneficiary institutions. Such training should address issues such as hacking techniques and the granting of access to facilities and equipment for non-employees without supervision. Policies should also be in place to direct people's actions (such as an access control policy stating who can access devices, who has what keys and what procedures should be followed if there is an intruder). For example, there should be a policy that states that before allowing anyone to access SANReN devices SANReN/TENET should be contacted to confirm their bona fides. If such measures were in place hackers would be unlikely to succeed in persuading people at the beneficiary institution to allow them to access the network. The guideline to address this threat is the same as the guideline proposed for addressing human error or failure.

| **Human Factor Threats** | **Applicability to SANReN** | **Existing SANReN Measures for Addressing the Threat** | **Recommendations for Addressing Addressing the Human Factor Threat in SANReN** |
|---|---|---|---|
| 1. Disgruntled employee | ✓ | ✘ | – SANReN/TENET management should employ people at SANReN beneficiary institutions to work specifically for SANReN/TENET.<br>– SANReN/TENET should develop an information security culture to shape and influence the behaviour of IT staff at the beneficiary institutions. |
| 2. Terminated employee | ✘ | ✘ | |
| 3. Human error or failure | ✓ | ✘ | – SANReN/TENET should establish a security education, training and awareness (SETA) programme for beneficiary institutions in order to address human factors such as human errors or failures within the SANReN network**.** |

|  |  |  |  |
|---|---|---|---|
| 4. Insufficient security awareness | ✓ | ✘ | – All SANReN beneficiary institutions should implement security awareness program that includes focus on issues relating to securing the SANReN network. |
| 5. Insufficient security training | ✓ | ✘ | – SANReN/TENET should implement a security training programme for beneficiary institutions in order to provide appropriate skills and knowledge for ensuring that the interface connecting to the SANReN network from the beneficiary institution is protected. |
| 6. Insufficient security education | ✓ | ✘ | – SANReN/TENET should ensure that the IT staff at beneficiary institutions have the qualifications, training, experience and certification required before granting access to SANReN devices. |
| 7. Lack of security policies and procedures | ✓ | ✘ | – SANReN/TENET should develop security policies that address operational concerns relating to the interface between the SANReN network and the beneficiary institution. |

| | | | |
|---|---|---|---|
| 8. Deliberate acts of theft | ✓ | ✗ | – SANReN/TENET should establish formal operational procedures specifying the roles and responsibilities of IT staff at beneficiary institutions. |
| 9. Hacker or Cracker | ✓ | ✗ | – SANReN/TENET should establish a security education, training and awareness (SETA) programme for beneficiary institutions in order to address human factors such as human errors or failures in the SANReN network |

Table 5-2: Summary of recommended guidelines

The focal point of these guidelines is people and their operational duties at the beneficiary institutions. Thus, the guidelines that have been drawn up can only be implemented among people. For example, a culture can only be developed where there are people to develop the culture.

People at beneficiary institutions will only know what is acceptable and unacceptable on the SANReN network when there are policies, procedures and rules in place to give them guidance and direction. Through the implementation of security education, training and awareness programmes SANReN could reduce the security breaches that may occur as a result of insufficient security awareness or training on the part of employees. With the help of SETA programmes, SANReN could improve employee awareness of the need to protect the network and develop the skills and knowledge related to secure behaviour.

## 5.6 Conclusion

This chapter identified and analysed threats related to the human factor. It further discussed whether or not the identified human factor threats are applicable to SANReN. Guidelines for addressing the human factor threats at SANReN beneficiary institutions were subsequently proposed. The following chapter will discuss the verification process for the proposed guidelines.

# CHAPTER 6: GUIDELINES FOR ADDRESSING HUMAN FACTORS IN THE SANREN NETWORK

## 6.1 Introduction

"*A guideline is a statement by which to determine a course of action. A guideline aims to streamline particular processes according to a set routine or sound practice" (US Department of Veterans Affairs, 2014)*.

The purpose of guidelines is to provide direction and guidance for the behaviour that should be displayed or the action that should be taken when dealing with a certain situation. Thus far, in the previous chapter (Chapter 5), this dissertation has conducted an analysis of the human factor threats to SANReN beneficiary institutions, and has recommended and proposed guidelines for addressing these threats. The proposed guidelines were developed in relation to the human factor threats that were identified and deemed to be applicable to the SANReN beneficiary network, thus the guidelines mainly address the operational concerns of the SANReN network at the beneficiary institutions. However, the outcome of this research could be applicable to most organizations; it does not only apply to the SANReN network. Addressing the human factor is the responsibility of every organization in order to manage organizational risks by assessing all the threats, vulnerabilities and then placing or improving controls for mitigating risks. This chapter will provide an overview of the proposed guidelines. It will also discuss the validation process of the proposed guidelines together with the feedback obtained during the validation process.

## 6.2 Overview of Guidelines

This section will provide a brief discussion of each of the proposed guidelines.

1. **SANReN/TENET management should employ people at SANReN beneficiary institutions to work specifically for SANReN/TENET**.

This guideline may be viewed as the cornerstone of all the guidelines proposed by this dissertation because it is only when there are people at the beneficiary institutions specifically dedicated to the SANReN network that the implementation of these guidelines can take place. As SANReN/TENET occasionally seeks assistance from the IT staff at the beneficiary institutions, there is a need for clear accountability and responsibility when giving network access to them. In order to properly secure the SANReN network therefore, SANReN/TENET management should invest more in the human side – it should employ its own staff at the beneficiary institution.

2. **SANReN/TENET should develop an information security culture to shape and influence the behaviour of IT staff at the beneficiary institutions**.

A culture can only be developed if there are people to implement the culture. Even with SANReN, an information security culture can only be developed if it has people (personnel) at the beneficiary institutions – without people there is no culture. It is important that SANReN/TENET management understands that no technology, security policies or procedures alone can predict security threats or know all the ways of interpreting them. A good solid security culture needs to be established in the beneficiary institutions.

3. **SANReN/TENET should establish a security education, training and awareness (SETA) programme for beneficiary institutions in order to address human factors such as human error or failures in the SANReN network**.

A SETA programme would build and strengthen the security defences of the SANReN network. It would help employees at the beneficiary institutions by placing security at the forefront of their minds when performing actions related to the SANReN network and would enable SANReN to hold beneficiary institutions accountable for their actions. SETA programmes are described by many researchers as the key to addressing human factor threats; therefore if SANReN establishes a SETA programme in beneficiary institutions such threats would be mitigated. In other words, establishing a SETA programme for SANReN institutions would provide the best return on investment because human related threats to the SANReN network would possibly decrease as a result.

4. **All SANReN beneficiary institutions should implement security awareness program that includes focus on issues relating to securing the SANReN network**.

The implementation of SANReN/TENET security awareness programmes would serve as the first line of defence for securing information systems and networks at beneficiary institutions. It would adjust people's attitudes and behaviours at beneficiary institutions to security and would also foster a security aware culture because people would be taught about SANReN policies and procedures, what they have to protect the network against and who to contact if a security breach occurs. Such awareness programmes would therefore help people at the beneficiary institutions to gain more understanding of the threats faced by networks and how they should respond to them.

5. **SANReN/TENET should implement a security training programme for beneficiary institutions in order to provide appropriate skills and knowledge for ensuring that the interface connecting to the SANReN network from the beneficiary institution is protected.**

The implementation of a security training programme could create another line of defence in addition to security awareness. Such a programme could be provided on the basis of the specific role that the individual plays. As the SANReN rollout continues to connect institutions around the country, it must be borne in mind that, at these institutions, there are different people with different levels of skills or competencies. Therefore, it can never be assumed that all institutions are competent or skilled enough to perform any task given by SANReN/TENET. For example, just because the NMMU network is operated by people with a high level of experience and skills, it does not mean that the WSU network operates at the same level. SANReN/TENET management should consider security training for beneficiary institutions to ensure that all institutions have received the same level of skills.

6. **SANReN/TENET should ensure that the IT staff at beneficiary institutions have the appropriate qualifications, training, experience and certification before granting access to SANReN devices.**

This guideline requires that SANReN provide beneficiary institutions with security education and that SANReN ensures that the people working with SANReN devices at the beneficiary institutions have adequate levels of skill, experience and qualifications. This is the best line of defence that SANReN could provide for beneficiary institutions and it would ensure that employees are knowledgeable, qualified and capable of performing any given task. People at beneficiary institutions should be provided with a more in-depth understanding of the security of the network, making it easier for them to respond effectively to network security threats.

7. **SANReN/TENET should develop security policies that address operational concerns relating to the interface between the SANReN network and the beneficiary institution.**

In order to give clear direction and guidelines to the beneficiary institutions policies must be in place, specifically operational policies. SANReN should at least provide clear guidelines on what is allowed and not allowed, and operational policy should clearly define the responsibilities, roles and authorisation for people at beneficiary institutions. Such policy should clearly state who is authorised to do what, and what access they are granted. It should also state that if something were to go wrong with the SANReN network who would be the first person to contact at the beneficiary institutions. The operational policy could also include the steps to be followed when reporting an incident or a threat, as well as the disciplinary action that will result should policy not be followed. The presence of this policy could also act as a deterrent for insider threats (disgruntled employee) because the insider would be well aware of the consequences that may arise as a result of his or her actions (termination or dismissal).

8. **SANReN/TENET should establish formal operational procedures specifying the roles and responsibilities of IT staff at beneficiary institutions.**

SANReN/TENET should develop operational procedures that guide beneficiary institutions with regard to their operational duties in the network. At beneficiary institutions formal procedures should be established to limit or restrict access and operational activities to authorised individuals only.

Figure 6-2 below shows a summary of the guidelines proposed by this dissertation for addressing the human factors in the SANReN network. It is important that the SANReN/TENET management carefully considers these guidelines. As the rollout of SANReN continues to other parts of the country, including the rural areas, consideration should be given to the operational procedures, policies and people in the SANReN network. It is therefore important that security education, training and awareness programmes are provided to the beneficiary institutions, and that formal procedures and operational security policies are drawn up.

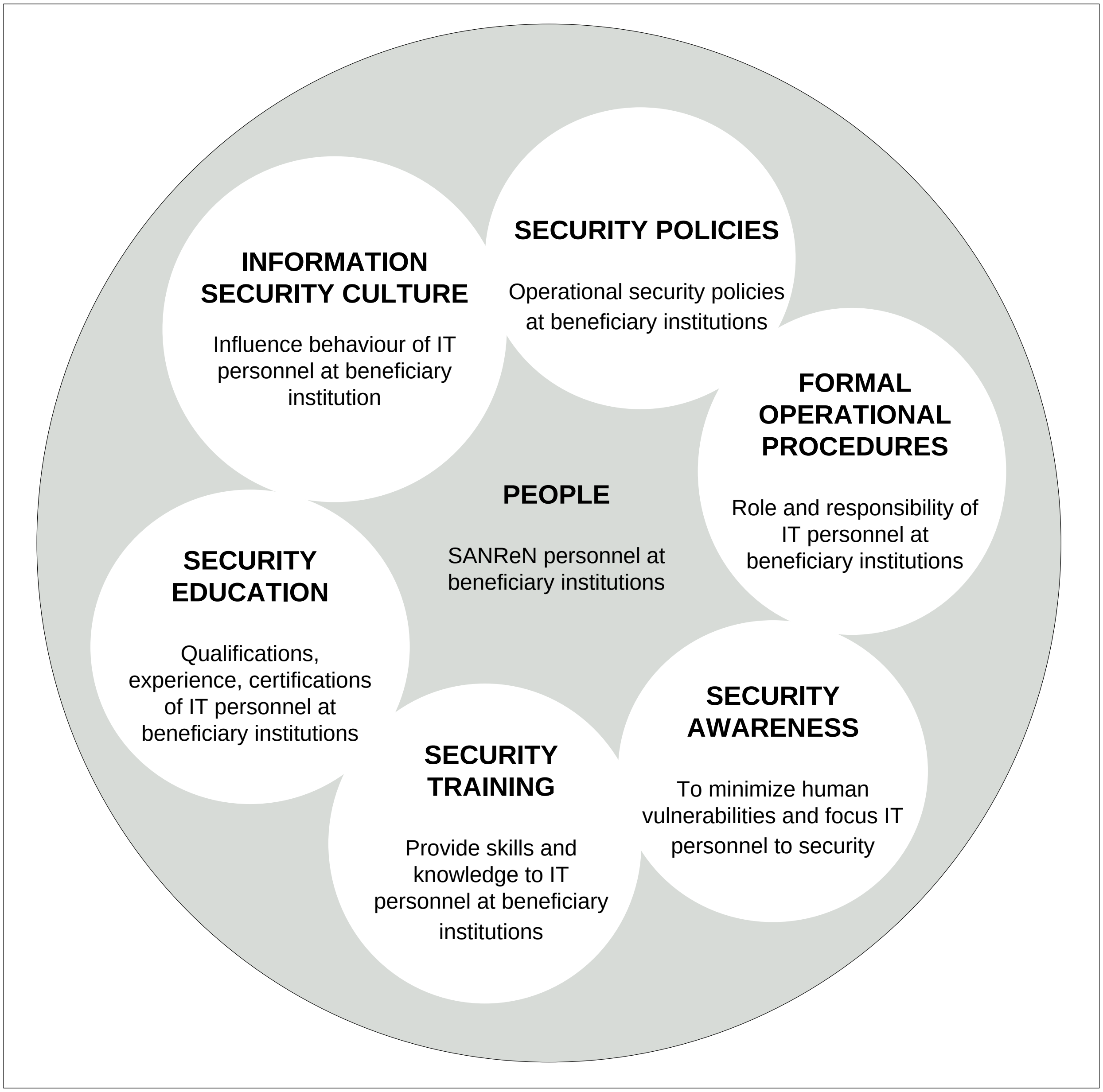
SECURITY POLICIES
Operational security policies at beneficiary institutions
INFORMATION SECURITY CULTURE
Influence behaviour of IT personnel at beneficiary institution
FORMAL OPERATIONAL PROCEDURES
Role and responsibility of IT personnel at beneficiary institutions
PEOPLE
SANReN personnel at beneficiary institutions
SECURITY EDUCATION
Qualifications, experience, certifications of IT personnel at beneficiary institutions
SECURITY AWARENESS
To minimize human vulnerabilities and focus IT personnel to security
SECURITY TRAINING
Provide skills and knowledge to IT personnel at beneficiary institutions

Figure 6-1: Guidelines for addressing the human factor threat in SANReN beneficiary institutions.

Beneficiary institutions should be given clearly specified roles and responsibilities. For example, it should be clearly documented in operational policies that at Rhodes University Mr

Smith is the contact person and that he is the one who has access to SANReN devices and is allowed to configure the device. Before Mr Smith is given access to the SANReN devices, a background check should be done on him to determine his level of skill, experience and knowledge, his qualifications and his capability in security the network. The following section will discuss how these guidelines were validated.

## 6.3 Validation of Guidelines

The guidelines for addressing the human factor threats in the SANReN beneficiary institutions were evaluated using expert review. Expert review is a validation process designed to gather the opinions of subject matter experts, it is a technique for collecting data directly from persons serving as subject-matter experts (Richey & Klein, 2007). Expert review can be used as the verification and evaluation technique of a particular design or output of the research (Willis, Schechter, & Whitaker, 1996).

In this study, the reviewers or experts were chosen based on their extensive experience in their line of work. The reviewers were network administrators at beneficiary institutions and SANReN and TENET engineers, these individuals were selected because of their direct involvement with the SANReN network. Initially, there were five experts' contacts for reviewing these guidelines, however only three responded, one from SANReN and two from the beneficiary institution. For the evaluation of these guidelines, a validation instrument was created as shown in appendix B and was distributed via email to the reviewers. The validation instrument provided the reviewers with a brief background of the study and presented each guideline. The reviewer's opinion was then gathered using a likert scale consisting of four levels of responses, namely strongly agree, agree, disagree and strongly disagree.

The usual neutral option was not included because the author wanted a clear and direct response from the experts.  A space for comments and suggestions was also provided after each guideline for the respondent to indicate why they agree or disagree with the guideline.

## 6.4 Feedback and Responses

The following section will discuss the feedback from the experts regarding the proposed guidelines as well as the researcher's response to this feedback.

Guideline 1: **SANReN/TENET management should employ people at SANReN beneficiary institutions to work specifically for SANReN/TENET.**

Regarding this guideline, we received three responses, strongly disagree, disagree and agree. The two experts disagreed with the guidelines because they viewed it as not financially feasible as "SANReN connects over 50 institutions with more than 200 sites connected to those beneficiary institutions". Financially it would be a challenge. The financial concerns that the experts are raising, have already been acknowledged in the dissertation (see section 5.5.1c). When the guideline was presented in Chapter 5, it was made clear that it would not be easily implemented as compared to other guidelines because of financial reasons.

One expert agreed with the guideline he stated, "Given the rapidly growing number of SANReN beneficiary institutions, it might be more practical to have staff available in various districts servicing multiple institutions". It can therefore be suggested that other models be explored such as having regional or district support person, where that individual could be responsible for 5-10 institutions per district.

Guideline 2: **SANReN/TENET should develop an information security culture to shape and influence the behaviour of IT staff at the beneficiary institutions.**

All the three experts agreed regarding this guideline, they selected (agree, agree and strongly agree). They indicated that it is a good suggestion and a role that is supposed to be played by an NREN (in this case by SANReN/TENET

Guideline 3: **SANReN/TENET should establish a security education, training and awareness (SETA) programme for beneficiary institutions in order to address human factors such as human error or failures in the SANReN network.**

Two of the reviewers agreed with this guideline and one disagreed stating that the human factors should be addressed through policies and procedures. It is the authors' opinion that, having policies and procedures in place does not guarantee that a person knows how to behave securely and adhere to policies. It cannot be assumed that people will know how to adhere to policies, they must be taught, trained and made aware of these policies. Additionally, the reviewer's alternative suggestion has already been proposed by guideline 7 of this dissertation.

Guideline 4: **SANReN/TENET should implement security awareness programmes for beneficiary institutions to focus their attention on securing the SANReN network.**

Two of the reviewers disagreed with this guideline; one of them stated, "SANReN has been intentionally designed as an "open" (non-restrictive) network. This does not mean that it is insecure but rather that it is not policed. It is not the beneficiary institutions' role to secure the SANReN network. Raising general IT security awareness level also focused on the beneficiaries' security and the implications of connecting to an "open" network will be more effective". The purpose of this guideline was not trying to focus on the entire SANReN network but to ensure that the SANReN interface or connection into the beneficiary institutions remains secure. Indeed, the author agrees that awareness programs should not only be the responsibility of the SANReN/TENET but also the responsibility of each beneficiary institution connected to SANReN. Therefore, this guideline will be phrased differently to clearly address the above concern. The guideline will therefore be re-phrased as the following: **All SANReN beneficiary institutions should implement security awareness program that includes focus on issues relating to securing the SANReN network.**

Guideline 5: **SANReN/TENET should implement a security training programme for beneficiary institutions in order to provide appropriate skills and knowledge of securing the network.**

Regarding this guideline two reviewers agreed with it, they viewed the guideline as something that could benefit both the connection "the interface" between SANReN and beneficiary institution, as well as the entire beneficiary networks. The third reviewer disagreed, but seems to misinterpret the scope of the suggestion. To address this misunderstanding this guideline will be rephrased to be more specific to “interface” between SANReN network and beneficiary institutions and not the entire beneficiary network. It will be rephrased as: **SANReN/TENET should implement a security training programme for beneficiary institutions in order to provide appropriate skills and knowledge for ensuring that the interface connecting to the SANReN network from the beneficiary institution is protected.**

Guideline 6: **SANReN/TENET should ensure that the IT staff at beneficiary institutions have the appropriate qualifications, training, experience and certification before granting access to SANReN devices.**

Two reviewers agreed with the guidelines and one disagreed stating that it will be very difficult to enforce and a qualification will not prevent security incidents. It is the author’s opinion that, even though qualification will not prevent people from malicious activities it will decrease the possibility of making mistakes because people will be highly knowledgeable about their roles and tasks.

Guideline 7: **SANReN/TENET should develop security policies that address operational concerns in SANReN beneficiary institutions.**

Two reviewers agreed with this guideline; however, one reviewer was not in agreement stating a valid reason that, SANReN has no jurisdiction except where TENET AUP is breached and it is the institutions responsibility to have its own information security policies. Alternatively, SANReN could assist the beneficiary institutions with best practice or code of conduct for the beneficiary institution interface, for example in the beneficiary institutions access to the SANReN devices must be clear. The guideline will be rephrased to focus more on the interface connection between the SANReN network and the beneficiary institutions. It will be rephrased as follows: **SANReN/TENET should develop security policies that address operational concerns relating to the interface between the SANReN network and the beneficiary institution.**

Guideline 8: **SANReN/TENET should establish formal operational procedures specifying the roles and responsibilities of IT staff at beneficiary institutions.**

All three reviewers agreed regarding this guideline, they viewed it as critical in providing stability of the network.

The feedback given by the reviewers in response to the suggested guidelines have been considered by the researcher and in response to this, three of the guidelines were re-worded in order to clearly clarify its scope and overall purpose. These changes have already been included in the guidelines as suggested in chapter 5.

Based on the feedback received from the reviewers, it can be concluded that the proposed guidelines are valid and relevant to the SANReN beneficiary network. The author acknowledges that some guidelines may not be quickly implemented because of finances. However, it is the author’s opinion that adhering to these guidelines will reduce threats posed to the SANReN network by the human factors.

## 6.5 Conclusion

This chapter provided an overview of the guidelines produced by this study and has emphasised the need for SANReN/TENET management to consider and implement these guidelines. The guidelines focus mainly on the operations of the SANReN network and not the technology – technology is fallible and because of its fallible nature, SANReN/TENET will not always be able to access its devices remotely to make configuration changes at beneficiary institutions. Therefore, at beneficiary institutions people are required to take over when SANReN/TENET has no access. When people take over device configuration, they must know what to do and how to do it. However, people are also fallible and they make mistakes. Therefore, security education, training and awareness should be provided for the beneficiary institutions together with formal procedures and operational security policies. These guidelines have been validated by means of expert reviews small changes were made to three guidelines to ensure that scope and purpose of the guidelines were clarified. The following chapter will conclude the dissertation.

# CHAPTER 7: CONCLUSION

## 7.1 Introduction

This dissertation focused on addressing the human factors that can threaten the SANReN network and has proposed guidelines for addressing the human factor related threats faced by SANReN beneficiary institutions. These guidelines were presented in Chapter 5 and were validated in Chapter 6. This chapter will conclude the dissertation by discussing the contributions made by the study and how the research objectives were achieved. The chapter will end with a discussion of the limitations of the study and the future research that could be conducted on this topic.

## 7.2 Discussion of Findings

The aim of this dissertation was to develop guidelines for addressing the human factor in the SANReN network of beneficiary institutions. Human factors are often overlooked by organisations even though humans are often cause of network security breaches or threats that result from human vulnerabilities. In addition, organisations generally invest more in technology than in the people using and maintaining this technology. Consequently, giving more attention to one element (technology) while ignoring the other (the human factor) could threaten the security of the network, because people have vulnerabilities and if these human vulnerabilities are not addressed the security of the network could at risk. From a technical point of view, the network engineers from SANReN and one of the beneficiary institutions (NMMU) regard this network as adequately secure. However, the current rollout of the SANReN network does not adequately address the human factor in information security. Since human factors are often the biggest threat to the security of a network, the SANReN network could be vulnerable to risks they pose.

The problem that this dissertation addressed was stated in section 1.8: *the rolling out of the SANReN network has not formally considered the information security risks posed by the human factors on the networks of the beneficiary institutions.* In order to address this problem the following research objectives were defined in section 1.9.

For addressing the identified problem, the primary objective of this study as presented in Chapter 1 (section 1.9) is to propose guidelines for addressing the information security related human factors in the rollout and continued management of the SANReN network.

In order to address this primary objective, secondary objectives were defined in chapter 1 (section 1.9) as listed below:

- *To analyse the current SANReN network in order to identify all human factors that might increase security risks to SANReN beneficiary institutions.*
- *To determine what the literature recommends with regard to addressing the human factors in information security.*
- *To investigate the role of information security education, training and awareness when addressing human factors in information security.*
- *To verify with the aid of an appropriate methodology the applicability of the proposed guidelines.*

The first secondary objective was *to analyse the current SANReN network in order to identify all human factors that might increase security risks to SANReN beneficiary institutions.* This research objective was addressed in Chapter 5 where the human factors applicable to the SANReN network were identified and analysed. These human factors were identified through an in-depth literature review and the current SANReN operation and management of the network at beneficiary institutions was examined to determine whether SANReN currently addresses the applicable human factors. The security policies governing the use of the SANReN network were then analysed in order to establish whether the human factors that could pose security risks to the SANReN network have been addressed in the policies. It was established that the SANReN does not currently address the human factor in the beneficiary institutions, as there are no measures are in place. As part of this study a peer reviewed paper on the analysis of the SANReN/TENET policies was published and presented at the HAISA 2014 conference (Appendix A).

The second objective was *to determine what the literature recommends with regard to addressing the human factors in information security.* This research objective was addressed in Chapter 3 where a detailed literature review was conducted on approaches to and ways of addressing the human factor in information and network security. It was established that the human factor could be addressed through the implementation of security education, training and awareness, formal operational procedures and operational security policies and the development of an information security culture.

The third objective was *to investigate the role of information security education, training and awareness when addressing human factors in information security.* This research objective was addressed in Chapter 3 where it was established that information security education, training and awareness plays a huge role in addressing the human factor threat. It was then emphasised that the SANReN network should start to address human-related threats through the provision of security education, training and awareness to the beneficiary institutions. Such provision would increase skills, decrease human vulnerabilities and increase the security of the SANReN network. Additionally, in Chapter 5 guidelines for information security education, training and awareness were proposed.

The fourth objective was *to verify with the aid of an appropriate methodology the applicability of the proposed guidelines.* This research objective was presented in Chapter 6. The proposed guidelines were evaluated by the SANReN engineer, the beneficiary institution network engineer and the TENET engineer. The proposed guidelines are as follows:

- SANReN/TENET management should employ people at SANReN beneficiary institutions to work specifically for SANReN/TENET.
- SANReN/TENET should develop an information security culture to shape and influence the behaviour of IT staff at the beneficiary institutions.
- SANReN/TENET should establish a security education, training and awareness (SETA) programme for beneficiary institutions in order to address human factors such as human error or failure in the SANReN network.
- SANReN/TENET should implement security awareness programmes for beneficiary institutions to focus their attention on securing the SANReN network.

- SANReN/TENET should implement a security training programme for beneficiary institutions in order to provide appropriate skills and knowledge for securing the network.
- SANReN/TENET should ensure that the IT staff at beneficiary institutions have appropriate qualifications, training, experience and certification before granting them access to SANReN devices.
- SANReN/TENET should develop security policies that address operational concerns in SANReN beneficiary institution.
- SANReN/TENET should establish formal operational procedures specifying the roles and responsibilities of IT staff at beneficiary institutions.

By addressing all four of the secondary objectives, it can therefore be argued that the primary research objective of this dissertation, which was to propose guidelines to address the information security related human factors in the rollout and continued management of the SANReN network, has been achieved.

## 7.3 Summary of Contribution

The SANReN network plays an important role in connecting South African researchers with other research institutions around the world, allowing collaboration with other countries and fostering economic growth. The SANReN network is one piece of the cyber infrastructure that attempts to close the digital divide in South Africa. Furthermore, the SANReN network contributes immensely in the economic development of South Africa and may be seen as a source of technological innovation for South African researchers. In spite of all the benefits that this network provides, it is still faced with the threats posed by the human factor, and this could represent the greatest security risk to the network. It is therefore very important that this factor is addressed by SANReN/TENET in order to ensure the continued availability of the network.

This dissertation has highlighted the importance of addressing the human factor in the SANReN network at the beneficiary institutions. It has established that there are currently no formal operational procedures and policies that specify roles and responsibilities at beneficiary institutions or address the human factor in the SANReN network. Therefore, guidelines for addressing the human factor threat at SANReN beneficiary institutions have been proposed. A peer reviewed paper on the lack of operational security policies at SANReN beneficiary institutions was published and presented at HAISA 2014 conference (Appendix A).

## 7.4 Limitations

This study focused in one beneficiary institution only because it was established in the early stages of the study that the problem to be solved by this research was similar in all the beneficiary institutions. For example, in all the beneficiary institutions the human factor had not been addressed, no security awareness programmes or training by SANReN/TENET was in place and no formal operational policies and procedures had been implemented by SANReN/TENET.

## 7.5 Future Research

This study proposed guidelines to assist in addressing the human factors in the SANReN network in order to ensure the continued availability of this network in South Africa. These guidelines could provide the initial step towards addressing human factor related threats at SANReN beneficiary institutions. However, in order for these guidelines to be useful and effective, they need to be implemented. The implementation of some of the proposed guidelines could take longer than others because of the lack of resources. For example employing people at SANReN beneficiary institutions to work specifically for SANReN/TENET could take longer than the implementation of formal operational procedures specifying the roles and responsibilities of IT staff at beneficiary institutions.

Future research could include an investigation of the way in which the guidelines should be implemented at all the beneficiary institutions; for example, specifying the steps that need to be followed in order to establish a security education, training and awareness (SETA) programme for beneficiary institutions to address human factors such as human error or failure in the SANReN network. Such research could also focus on the content that such programmes should teach people at beneficiary institutions and how they should be taught it.

When all these guidelines have been implemented at the beneficiary institutions, another possible future research study would be to investigate human factor related incidents before and after the implementation of the guidelines.

## 7.6 Final Word

Technical controls should not be the only concern when addressing security on the network – the human factor also needs to be considered. Accordingly, the SANReN network may be vulnerable to risks posed by the human factor despite the presence of technological controls. If the human factor is not adequately addressed it could result in vulnerabilities in the network, which if exploited could compromise the security of the network. This study established that people are the cornerstone of information security and network security. If the cornerstone (people) is not securely laid, the entire building (network) will collapse. Therefore, in order for people behave securely at beneficiary institutions they need to be taught how to behave securely – this can never be assumed. Clear roles and responsibilities, procedures and operational policies must be in place in beneficiary institutions in order to govern the use of the SANReN network.

# REFERENCES

Abou El Kalam, A., Deswarte, Y., Baïna, A., & Kaâniche, M. (2009). PolyOrBAC: A security framework for Critical Infrastructures. *International Journal of Critical Infrastructure Protection*, *2*(4), 154–169. doi:10.1016/j.ijcip.2009.08.005

Ahmed, M., Sharif, L., Kabir, M., & Al-maimani, M. (2012). Human Errors in Information Security. *International Journal of Advanced Trends in Computer Science and Engineering*, *1*(2278), 82–87.

Alavi, R., Islam, S., Jahankhani, H., & Al-Nemrat, A. (2013). Analyzing Human Factors for an Effective Information Security Management System. *International Journal of Secure Software Engineering*, *4*(1), 50–74.

Andress, J. (2011). *THE BASICS OF INFORMATION SECURITY*. (A. Ward & H. Scherer, Eds.). Syngress.

Applegate, S. D. (2009). Social Engineering: Hacking the Wetware! *Information Security Journal: A Global Perspective*, *18*(1), 40–46. doi:10.1080/19393550802623214

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report*, *13*(4), 195–201.

Ashton, K. (2009). That'Internet of Things'Thing. *RFID*. Retrieved from http://www.rfidjournal.com/articles/view?4986

ASPIRE. (2012). *The Future Roles of NRENs*.

Baars, H., Hintzbergen, J., Hintzbergen, K., & Smulders, A. (2010). *Foundations of Information Security: Based on ISO27001 and ISO27002*. (S. Newton, Ed.). ZAltbommel: Van Haren Publishing.

Bacik, S. (2008). *Building an Effective Information Security Policy Architecture*. United States of America: CRC Press.

Baker, W. H., & Wallace, L. (2007). Is Information security under control?: Investigating quality in information security management. *Security & Privacy, IEEEE*, *5*(1), 36–44.

Ballad, B., Ballad, T., & Banks, E. (2010). *Access Control, Authentication, and Public Key Infrastructure*. Canada: Jones and Bartlett Leaning.

Cardenas, A. A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009). Challenges for Securing Cyber Physical Systems.

Cavelty, M. D. (2007). *Critical Information Infrastructure: Vulnerabilities, Threats and Responses*.

Ciampa, M. (2012). *Security+ Guide to Network Security Fundamentals*. (D. Garza, S. Helba, & D. Kaufmann, Eds.) (4th ed.). Bonston: Course Technology.

Cisco. (2008). *Data Leakage Worldwide : The High Cost of Insider Threats* (pp. 1–6).

Cisco. (2011). *The Cisco Connected World Technology Report* (pp. 1–36). Retrieved from http://www.cisco.com/en/US/solutions/ns341/ns525/ns537/ns705/ns1120/CCWTR-Chapter1-Report.pdf

Cisco. (2012). Cisco CCNA Exploration Network fundamentals. Retrieved from www.r125cnap1.ac.za

Clemente, D. (2013). *Cyber Security and Global Interdependence: What Is Critical?*

Cole, E. (2009). *Network Security Bible* (2nd ed.). Wiley.

Cole, E., & Ring, S. (2005). *Insider Threat*. (G. Byrne & M. Melani, Eds.) (1st ed.). Canada: SyngressPublishing Inc.

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, *14*(4), 186–196. doi:10.1016/j.istr.2010.04.004

Council National Research. (2002). *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. Washington, D.C.: The National Academies Press.

Creswell, J. W. (2009). *Research Design*. Thousand Oaks, California: SAGE.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, *20*(1), 79–98. doi:10.1287/isre.1070.0160

DANTE. (2014). What is DANTE. Retrieved from http://www.dante.net/pages/faqs.aspx

Deloitte. (2009). *Protecting what matters The 6th Annual Global Security Survey*.

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, *28*(3-4), 189–198. doi:10.1016/j.cose.2008.11.007

Douligeris, C., & Serpanos, D. N. (2007). *Network Security: Current Status and Future Directions*. (C. Douligeris & D. N. Sepanos, Eds.). John Wiley & Sons.

Dunn, M., & Wigert, I. (2004). *CIIP Handbook 2004 CIIP Handbook 2004*. (A. Wenger & J. Metzger, Eds.).

Dyer, J. (2009). *The Case for National Research and Education Networks ( NRENs )*.

Ernst & Young. (2008). *Moving beyond just compliance*. *Behavioral healthcare* (Vol. 26).

FBI. (n.d.). *Recent insider threat cases*. Retrieved from http://www.fbi.gov

FBI. (2007). *Disgruntled former employee pleads guilty to unauthorized access of compant computers*. Chicago. Retrieved from http://www.justice.gov

Fraser, B. (1997). *Site security handbook*.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983–988. doi:10.1016/j.cose.2012.08.004

Furnell, S., & Warren, M. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium? *Computers & Security*, *18*, 28–34.

Gonzalez, J. J., & Sawicka, A. (2002). A Framework for Human Factors in Information Security.

Goodman, S. E. (2008). Critical Information Infrastructutre Protection. In Centre of Excellence Defence Against Terrorism (Ed.), *Proceedings of the NATO Advanced Research Workshop on Responses to Cyber Terrorism*. Ankara, Turkey: IOS Press.

Gray, D. E. (1999). The Internet in lifelong learning: liberation or alienation? *International Journal of Lifelong Education*, 119 – 126. doi:10.1080/026013799293874

Grobler, M., & Bryk, H. (2010). Common Challenges Faced During the Establishment of a CSIRT. *IEEE*, 2–7.

Hamed, H., & Al-Shaer, E. (2006). Taxonomy of Conflicts in Network Security Policies, 134–141.

Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers & Security*, 31–42.

Hight, S. D. (2005). The importance of a security , education , training and awareness program, *27601*(November), 1–5.

Hinson, G. (2014). *Human factors in information security* (pp. 1–6).

Holton, C. (2009). Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem. *Decision Support Systems*, *46*(4), 853–864. doi:10.1016/j.dss.2008.11.013

Huang, D.-L., Patrick Rau, P.-L., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, *69*(12), 870–883. doi:10.1016/j.ijhcs.2011.07.007

Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, *29*(3), 221–232. doi:10.1080/01449290701679361

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, *13*(4), 247–255. doi:10.1016/j.istr.2008.10.010

Hunton, P. (2011). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital Investigation*, *7*(3-4), 105–113. doi:10.1016/j.diin.2011.01.002

Hyslop, M. (2007). *Critical Information Infrastructures: Resilience and Protection*. United Kingdom: Springer.

Internet World Stats. (2012). The Digital Divide. Retrieved from http://www.internetworldstats.com/links10.htm

Internet World Stats. (2014). World Internet Usage and Population Statistics. Retrieved October 30, 2014, from http://www.internetworldstats.com/stats.html

ISO/IEC 27002. (2007). ISO/IEC 27002, *35*.

ISO/IEC 27032. (2012). *INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Guidelines for cybersecurity*. Retrieved from ISO/IEC

Jaume-Rajaonia, S., Veiga, P., Santos, L., Bøge, K., Passchier, S., Kisfaludi, G., … Devester, M. (2003). *Report on examples of extension of research networks to education and other user communities*.

Jones, A., & Colwill, C. (2008). Dealing with the Malicious Insider. In *Australian Information Security Management Conference*.

Jungck, P., & Simon, S. Y. S. (2004). Issues in High-Speed Internet Security. *IEEE*.

Kermarrec, A. (2013). Towards a personalized Internet : a case for a full decentralization. *Mathematical , Physical & Engineering Sciences*, (February).

Kim, W., Jeong, O.-R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, *36*(3), 675–705. doi:10.1016/j.is.2010.11.003

Koroliov, V., Turesson, M., & Brolin, O. (2009). *What is your password? Assessing information security awareness among employees in an organization*.

Kotzanikolaou, P., Theoharidou, M., & Gritzalis, D. (2013). Assessing n-order dependencies between critical infrastructures. *Int. J Critical Infrastructure*, *9*, 93–110.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists. *Applied Ergonomics*, *38*(2), 143–54.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, *28*(7), 509–520. doi:10.1016/j.cose.2009.04.006

Krause, M., & Tipton, H. F. (2004). *Handbook of Information Security Management*. (H. F. Tipton & M. Krause, Eds.) (5th ed.). Washington, D.C.: CRC Press LLC.

Kraut, R., Patterson, M., Lundmark, V., Mukopadhyay, T., & Scherlis, W. (1998). Internet paradox. *American Psychologist*, *53*(9), 1017–1031.

Kreitner, R., & Kinicki, A. (1995). *Organizational behavior*. Chicago.

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology* (2nd ed., Vol. 13, pp. 392–394). Thousand Oaks, CA: SAGE Publications.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, *27*(5-6), 224–231. doi:10.1016/j.cose.2008.05.006

Kritzinger, E., & von Solms, S. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 1–15.

Kuun, C., Wright, C., & Staphorst, L. (2013). *SANReN Current and Future Developments*. South Africa.

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*(1), 4–13. doi:10.1108/09685221011035223

Lazer, D., Brewer, D., Christakis, N., Fowler, J., & King, G. (2009). *Life in the network: the coming age of computational social science* (Vol. 323, pp. 721–723).

Lehto, M. R., & Landry, S. J. (2013). *Introduction to Human Factors and Ergonomics for Engineers*. (G. Salvendy, Ed.) (2nd ed.). United States of America: CRC Press.

Licht, D. M., Polzella, D. J., & Boff, K. R. (1989). *Human Factors, Ergonomics and Human Factors Engineering: An Analysis of Definitions*.

Lundy, O., & Cowling, A. (1996). *Strategic Human Resource Management*. London: Routledge.

Martin, D. (2012). *Tertiary Education and Research Network of South Africa NPC* (pp. 1–4). Retrieved from http://www.tenet.ac.za

Martin, D. H. (2012). *Using NREN capacities to extend and enhance UbuntuNet* (pp. 3–7). South Africa.

Meraka Institute. (2007). African Advanced Institute for Information and Communication Technology. Retrieved from http://www.meraka.org.za/Faqs

Mertens, D. M. (1998). *Research methods in education and psychology: Integrating diversity with quantitative and qualitative approaches*. SAGE Publications.

Mitnick, K. D., Simon, W. L., & Wozniak, S. (2002). *The Art of Deception: controlling the human element of security*. (C. Long, N. Stevenson, & J. Atkins, Eds.). Robert Ipsen.

Moller, K. (2007). Setting up a Grid-CERT : experiences of an academic CSIRT. *Campus-Wide Information Systems*, *24*(4), 260–270. doi:10.1108/10650740710834644

Monk, T., van Niekerk, J., & von Solms, R. (2010). Sweetening the medicine: educating users about information security by means of game play. *SAICSIT*, 193–200. doi:10.1145/1899503.1899525

Mooi, R. (2012a). *Introduction to CSIRTs* (p. 5). Retrieved from http://www.sanren.ac.za/wp-content/uploads/2012/11/SANReN_CSIRT_Introduction.pdf

Mooi, R. (2012b). *Security Incident Response for the South African NREN* (p. 9). Retrieved from http://www.sanren.ac.za/wp-content/uploads/2012/11/IRT_background_survey_problem_SANReN.pdf

Mooi, R. (2013). *SA NREN CSIRC Model* (p. 14). Retrieved from http://www.sanren.ac.za/wp-content/uploads/2013/05/SA_NREN_CSIRC_Model-Published.pdf

NATO. (2012). *National Cyber Security Framework Manual*. Tallinn. doi:9789949921119

NIST 800-16. (1998). *Information Technology Security Training Requirements : A Role- and Performance-Based Model*. (M. Wilson, Ed.).

NIST 800-16. (2013). *NIST Special Publication 800-16 A Role-Based Model for Federal Information Technology / Cyber Security Training* (Vol. 1). United States.

NIST 800-30. (2002). *Risk Management Guide for Information Technology Systems* (Vol. 30). United States.

NIST 800-30. (2012). *Guide for Conducting Risk Assessments*. United States.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, 1–8. doi:10.1016/j.cose.2012.04.004

Parsons, K., Mccormac, A., Butavicius, M., & Ferguson, L. (2010). *Human Factors and Information Security : Individual , Culture and Security Environment*. Edinburgh.

Photopoulos, C. (2011). *Managing Catastrophic Loss of Sensitive Data: A Guide for IT and Security ... By , 2011*. Syngress.

Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638–646. doi:10.1016/j.cose.2004.10.006

Posthumus, S., Von Solms, R., & King, M. (2010). The board and IT governance : The what , who and how. *South African Journal of Business Management (S AFR J BUS MANAG )*, *41*(3), 23–32.

PricewaterhouseCoopers. (2010). *Protecting your business*. *Veterinary Record* (Vol. 122). doi:10.1136/vr.122.17.421

Raval, V., & Fichadia, A. (2007). *RISK, CONTROLS, AND SECURITY*. (C. DeJohn, M. Bonadeo, & V. A. Vergas, Eds.). Don Fowley.

Richey, R. C., & Klein, J. D. (2007). *Design and Development Research: Methods, Strategies, and Issues*.

Ritchey, R. W., & Ammann, P. (2000). Using Model Checking to Analyze Network Vulnerabilities. *IEEE*.

Robert, W., & Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through Situational Crime Prevention. *Communication of ACM*, *52*(9). doi:10.145/1562164.1562198

Salvendy, G. (2012). *Handbook of Human Factors and Ergonomics* (4th ed.). Hoboken, New Jersey: John Wiley & Sons.

SANReN. (2012). *About SANReN* (pp. 1–11).

SANReN. (2013a). *About SANReN* (pp. 1–10).

SANReN. (2013b). Information and Communication Technology Services. Retrieved April 12, 2013, from http://www.icts.uct.ac.za/modules.php?name=News&file=article&sid=5533

SANReN. (2014). SANReN Overview. Retrieved April 10, 2013, from http://www.sanren.ac.za/overview

SANS. (2010). *SANS Institute InfoSec Reading Room. Humans the Ovelooked Asset*.

Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report*, *15*(3), 112–133. doi:10.1016/j.istr.2010.11.002

Sasse, M. A., Ashenden, D., Lawrence, D., Coles-kemp, L., Fléchais, I., & Kearney, P. (2007). *HUMAN FACTORS WORKING GROUP WHITE PAPER Human Vulnerabilities in Security Systems* (pp. 1–10).

Shaw, E. D., Post, J. M., & Ruby, K. G. (1999). Inside the Mind of the Insider. Retrieved March 08, 2009, from www.securitymanagement.com

Singh, B. (2009). *Network Security and Management* (2nd ed.). New Delhi: PHI Learning Private Limited.

Siponen, M., Mahmood, A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217–224. doi:10.1016/j.im.2013.08.006

Snedaker, S. (2006). *IT Security Project Management*. (R. Rogers, Ed.). Canada: Syngress Publishing.

Stephens, K. (2010). *The Cyberspace Insider Threat* (pp. 1–5).

Swain, A. D., & Guttman, H. E. (1983). *Handbook of human reliability analysis with emphasis on nuclear power plant applications.* Washington, D.C.

TERENA. (2009). *TERENA COMPENDIUM*. Retrieved from www.terena.org/compendium

TERENA. (2010). Research and education networking FAQ. Retrieved from http://www.terena.org/activities/development-support/r+e-faq/general.html

TERENA. (2012). *TERENA COMPENDIUM of National Research and Education Networks in Europe*. Amsterdam, Netherlands.

TERENA. (2013). *TERENA COMPENDIUM of National Research and Education Networks in Europe*. Amsterdam, Netherlands.

Theoharidou, M., Xidara, D., & Gritzalis, D. (2008). A CBK for Information Security and Critical Information and Communication Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, *1*, 81–96. doi:10.1016/j.ijcip.2008.08.007

Thomson, K. L., & von Solms, R. (2006). Towards an Information Security Competence. *Computer Fraud & Security*, 11–15.

Thomson, K., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, (10), 7–11.

U.S Department of Veterans Affairs. (2014). One-VA Technical Reference Model v14.10. Retrieved October 04, 2014, from http://www.va.gov/trm/TRMGlossaryPage.asp

UbuntuNet Alliance. (n.d.). TENET South Afrca. Retrieved March 03, 2013, from www.ubuntunet.net

Van Niekerk, J. F., & von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security - COMPSEC*, *29*(4), 476–486.

Veiga, D. a., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207. doi:10.1016/j.cose.2009.09.002

Von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371–376. doi:10.1016/j.cose.2004.05.002

Von Solms, R., Thomson, K.-L., & Maninjwa, P. M. (2011). Information security governance control through comprehensive policy architectures. *Information Security South Africa (ISSA)*, 11–16.

Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. doi:10.1016/j.cose.2013.04.004

Von Solms, R., & von Solms, B. (2004). From policies to culture. *Computers & Security*, *23*(4), 275–279. doi:10.1016/j.cose.2004.01.013

Von Solms, R., & von Solms, B. S. . (2006). Information Security Governance: A model based on the Direct–Control Cycle. *Computers & Security*, *25*(6), 408–412. doi:10.1016/j.cose.2006.07.005

Von Solms, R., & von Solms, S. H. (2009). *Information Security Governance*. Springer. doi:10.1007/978-0-387-79984-1

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191–198. doi:10.1016/j.cose.2004.01.012

Wamala, F. (2011). *THE ITU NATIONAL CYBERSECURITY STRATEGY GUIDE*.

Wellman, B., Quan-haase, A., Boase, J., & Chen, W. (2002). Examining the Internet in Everyday Life. In *Euricom Conference on e-Democracy* (pp. 1–18). Netherlands.

Whitman, M. E., & Mattord, H. J. (2010). *MANAGEMENT OF INFORMATION SECURITY*. (D. Garza, S. Helba, & M. Bellegarde, Eds.) (4th ed.). Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security*. (D. Garza, S. Helba, & B. Marah, Eds.) (4th ed.). Boston: Course Technology.

Williams, P. A. H. (2008). In a “trusting” environment, everyone is responsible for information security. *Information Security Technical Report*, *13*(4), 207–215.

Willis, G. B., Schechter, S., & Whitaker, K. (1996). A COMPARISON OF COGNITIVE INTERVIEWING, EXPERT REVIEW, AND BEHAVIOR CODING: WHAT DO THEY TELL US?, (1994), 28–37.

Wood, C. C. (2002). The Human Firewall Manifesto. *COMPUTER SECURITY JOURNAL*, *18*, 15–18.

Yin, R. K. (2014). *Case Study Research* (5th ed.). Thousand Ooaks, CA: SAGE publication.

# APPENDIX A:

# HAISA PRESENTED AND PUBLISHED

# Exploring the Human Dimension in the Beneficiary Institutions of the SANReN Network

Y. Mjikeliso, J.F. Van Niekerk and K.L. Thomson

Institute for ICT Advancement, Port Elizabeth, South Africa
e-mail: {s209039445@; Johan.vanniekerk; Kerry-lynn.thomson}@nmmu.ac.za

## Abstract

One of the factors that play a major role in information security is people. People are the drivers of most processes and procedures in information security. However, many researchers agree that human aspects are not given enough attention; more focus is given to the technical security. This is especially true in the security of the underlying network infrastructure which is often seen as a technical issue and not a human issue. It is senseless to have good solid technical security without considering humans because most security breaches are caused by human mistakes. Regardless of all the technical and physical controls implemented for network security, which underpins information security, there will always be human vulnerabilities to the security of the network. Therefore, attention should be given to the human factors as it is widely acknowledged as the biggest vulnerability in network security, which impacts on information security. In South Africa there is an important network infrastructure known as the South African National Research Network (SANReN) which provides vitally important Internet access to research and educational facilities throughout South Africa. The SANReN network has the potential to provide many opportunities and benefits to the people of South Africa. It is therefore extremely important that the SANReN network is highly secured at all times in order to ensure continued availability of the network. This paper will focus on human factors that could affect the security of the SANReN beneficiary networks. Policies governing the use of the SANReN network will be investigated in order to establish whether human factors, which could pose security risks to the SANReN network, have been addressed in the policies.

## Keywords

Human Factors, SANReN Beneficiary Networks, Policies

## 1. Introduction

The management of information security depends on technology, processes and people. However, more emphasis is often placed on strengthening the technological aspects and processes, while less attention is given to the human aspects (Ashenden, 2008). Even security surveys commonly acknowledge that the human aspects, such as policy, training and education, are more likely to be given less attention than the technical controls, such as firewalls, antivirus and intrusion detection (Furnell & Clarke, 2012). Regardless of all the technical and physical controls implemented for network security, which underpins information security, there will always be human vulnerabilities to the security of the network. Information security is about the protection of information and its critical characteristics (confidentiality, integrity, availability), as well as the systems and hardware that use, store and transit that information (Whitman & Mattord, 2011). Network security is one underlying component of information security without which it may be difficult to achieve information security. This paper will firstly determine whether human factors are considered or addressed in the security of the SANReN beneficiary networks. The paper presents content analysis of the existing policies used to govern the SANReN network, in order to determine whether human factors which could affect the security of the SANReN network have been addressed in the policies.

## 2. Methodology

The paper utilises a combination of content analysis of policies, as well as interviews with SANReN network engineers and a network administrator from one of the SANReN beneficiary institutions. All current policies governing the SANReN network were gathered by collecting documents from the TENET (discussed in Section 2.2) website, through email correspondence with SANReN personnel, as well as through interviews with network administrators at beneficiary institutions. The main focus of the content analysis of the policies was to identify whether or not human factors or human aspect issues were currently being addressed within the SANReN policies.

## 3. NREN

A National Research and Education Network (NREN) is a specialised Internet service provider for the research and educational communities within a country (TERENA, 2010). It provides research institutions and educational institutions with services and access to the Internet. Other than just providing connectivity to the Internet, the NREN should also provide a number of important services such as a Network Operations Centre, performance monitoring and management, incident response (TERENA, 2009). The way in which the NRENs are managed from country to country differs, as the organizational and ownership model for each NREN varies (TERENA, 2010).

### 3.1. SANReN

SANReN is a high speed communication network that is designed primarily for research institutions and organizations. The main purpose of the SANReN network is to provide the South African research institutions and organizations with Internet access and related services, as well as connecting them to research networks all over the world. The SANReN network together with the Centre for High Performance Computing (CHPC) and Very Large Databases (VLDB) create the key components of the cyber infrastructure in South Africa (Meraka Institute, 2007). The major role players of the SANReN network are:

- Department of Science and Technology (DST)
- Council for Science and Industrial Research (CSIR) Meraka Institute
- Tertiary Education and Research Network of South Africa (TENET)
- SANReN beneficiary institutions

The SANReN network is a South African DST project, implemented by the CSIR through the Meraka Institute (Meraka Institute, 2007). The project is part of the South African government's approach to cyber infrastructure to ensure the successful participation of South African researchers in global knowledge (SANReN, 2014). The CSIR is the governing body of the SANReN network and the operational services of the SANReN network to all beneficiary institutions is provided by TENET on behalf of the CSIR (SANReN, 2014). A *beneficiary institution* is an institution that is defined by the DST as institutions that are allowed to be connected to the SANReN network. These beneficiary institutions are the current TENET institutions, such as universities and research councils (SANReN, 2014). The following subsection will provide more detail on TENET which is one of the SANReN role players.

### 3.2. TENET

TENET is a specialized ISP for higher education and research sector, which provides Research and Education Networking services "REN services" like Internet and related services to about 160 campuses of 54 institutions, including universities, research councils and other associated institutions (UbuntuNet Alliance, n.d.). All the public universities and science councils in South Africa qualify to be a part, or a member, of the TENET network (Martin, 2012). The South African NREN is formed by SANReN together with TENET. The roles and responsibility of the South African NREN (SANReN) are given to both the SANReN team and to the TENET team. The SANReN team build the network and the TENET team operates the network (Martin, 2012). The following subsection will focus on how the SANReN network is being rolled out.

### 3.3. SANReN Network Implementation

The SANReN project is being rolled out in a phased manner and will eventually connect up to 204 sites across South Africa, and connecting over 3 000 education and research organizations from all over the world (SANReN, 2014). The South African universities, research councils such as the CSIR, National Research Foundation (NRF) , and various other research institutes are the beneficiary institutions of SANReN (SANReN, 2014). These beneficiary institutions form the SANReN national network backbone. The SANReN network backbone consists of a 10Gpbs 7-stretch backbone ring between the South African major cities. The SANReN Point of Presences (PoPs), are placed in all the connected institutions. The rolling-out of SANReN is still progressing to other beneficiary institutions and will eventually also connect remote towns (Martin, 2012). SANReN has the potential to provide many opportunities and benefits to the people of South Africa. Rural areas will have increased accessibility to the Internet, which could help in addressing the digital divide (SANReN, 2012). The SANReN network is one of the cyber infrastructures attempting to close the digital gap between those who have access to the Internet and those who do not have, and will connect a wide variety of people. Therefore, it is important that the SANReN network is secured at all times in order to ensure the continued availability of the network.

## 4. Securing the SANReN Network

Many NRENs have Computer Security Incident Response Teams (CSIRTs) in place in order to respond to security incidents of the network (Moller, 2007). As a result, the SANReN team is also in the process of establishing a SANReN / TENET CSIRT team which will be responsible for managing the security incidents of the SANReN network. CSIRT is a team of people who are responsible for receiving and responding to network security incident reports and activities (Mooi, 2013). The need for the SANReN / TENET CSIRT was identified through a survey conducted in May 2012 (Mooi, 2012a). The survey was sent out to all the beneficiary institutions of the SANReN network. The purpose of the survey was to investigate whether the beneficiary institutions would be interested in an incident response team, as there is no central point, or a central managing party, for incident handling on the SANReN network at present. The TENET NOC (Network Operations Centre) is responsible for incident handling. However, there may be restricted resources and the TENET team may lack effectiveness since they may be the only ones responsible for incident handling (Mooi, 2012a). When the SANReN / TENET CSIRT team is established it will be responsible for protecting against all types of malicious activities on the SANReN network such as; spam, denial of service attacks or hacking attempts. Their responsibility will be to receive, review and respond to the network security incidents (Mooi, 2012b). From a technical point of view, the SANReN network may be more secure as a result of the SANReN / TENET CSIRT team. However technical controls should not be the only concern for addressing security on the SANReN network – human factors should also be of concern, as will be discussed in section 4. The SANReN network may be vulnerable to risks posed by human factors even if technological controls exist on the network.

## 5. Human Factors on the SANReN Network

"Don't rely on network safeguards and firewalls to protect your information. Look to your most vulnerable spot. You'll usually find that vulnerability lies in your people" (Mitnick & Simon, 2002). There are technical solutions for solving what is seen as a technical issue. However, having technical solutions can create a false perception of security. Even though technical security is very important and without it networks would be vulnerable, there is still a vulnerability that remains because of negligence and the malicious acts of human beings. Negligence, ignorance, anger or even curiosity are human elements which can increase security incidents (PricewaterhouseCoopers, 2010). Human beings are a more challenging problem to address because there is no easy way to target them; there are no product-based solutions for people, unlike technical solutions (Furnell & Clarke, 2012).

Many researchers agree that human factors are one of the most significant vulnerabilities in information security and are often overlooked in organizations (Thomson & von Solms, 2006; Kraemer & Carayon, 2007). People are said to be the greatest threat to information security, and are often the 'point of failure', whether intentionally or through negligence or a lack of knowledge. However, people could represent the key element in achieving security (van Niekerk & von Solms, 2010;

Furnell & Clarke, 2012).Human factors play a role on the SANReN network just like in any other network. The rolling out of the SANReN network has started for various beneficiary institutions and a number of people have been involved with this project. There are people involved in configuring the network devices, creating policies and using the network as end-users. It is important to understand that, by nature, people have limited attention and accuracy - they make mistakes and errors (Ashton, 2009). Therefore, SANReN must properly address the human vulnerabilities. The mistakes and errors that people make could result in security vulnerabilities (Kraemer, Carayon, & Clem, 2009). The greatest vulnerability to the security of the SANReN network may be the people that the network connects or the employees.

An interview was conducted with one of the network administrators at the Nelson Mandela Metropolitan University (NMMU), which is a beneficiary institution of the SANReN network. The interview was conducted in order to identify whether issues related to human factors could pose security risks to the SANReN network. The network administrator was completely certain and confident about the technical and physical security of SANReN network. "We believe that the management of SANReN is being done by some of the best IT professionals in South Africa, so in my opinion, I believe that the network configuration is as secure as necessary". According to the network administrator, the beneficiary institutions host the network devices and the TENET team remotely accesses the devices or sends someone from SANReN / TENET when they need to make configuration changes on the network devices. There are no people working for SANReN / TENET at the beneficiary institutions and the connected institutions have no management or configuration access to the SANReN networking devices. However, the network administrator also mentioned an incident where on one or two occasions the SANReN network administrators from TENET managed to lock themselves out of the remote configuration session. They required local assistance from IT staff at the NMMU and the local IT staff had to make the configuration changes to the network device of SANReN. The fact that the TENET people were able to lock themselves out of the configuration session indicates there was a human mistake or error. Therefore, through this human error, members of the local IT staff at the NMMU were given access to network devices that they should not usually have access to. From this incident it could be implied that even though the network might be seen as technically and physically secured, human factors could be the weakest link in the security of the SANReN network.

For example, here in South Africa there are institutions from disadvantaged areas which might lack highly trained IT professionals. What if a low-level skilled individual was asked to perform these changes on the SANReN network devices and ended up misconfiguring the devices creating more problems on the network? Having been granted access to the networking devices and, for example, knowingly or unknowingly connecting a device which contains viruses and worms which may be distributed throughout the network could have a severe impact on network security. Therefore, the SANReN / TENET network may be exposed to many security risks by allowing access to the wrong individuals. SANReN / TENET are not aware of how skilled or qualified the individuals are that they are giving access to the network. This may present a good opportunity for an insider threat to manifest. An insider threat poses a security risk to the network because of the legitimate access to facilities, information, and knowledge of an organization and the location of valuable assets (Williams, 2008).

Another possible threat would be to apply a security related patch to incorrect software or failure to secure the correct port making it a target for network attackers. Most network attackers usually start by looking for vulnerabilities or weaknesses of the individual or computer they can communicate with on the network targeted. Many software packages will never be free of vulnerabilities because of human errors (Grobler & Bryk, 2010). Any network will have some level of vulnerabilities as it is impossible to completely eliminate vulnerabilities (Ritchey & Ammann, 2000). It is, therefore, very important that networks such as SANReN properly address the vulnerability of human factors. In other words, their end-users and IT staff must know their roles and responsibilities and adhere to correct behaviour to protect the network. In order for people to adhere to correct behaviour there must be organizational policies from management dictating the appropriate behaviour of the employees (von Solms & von Solms, 2004). As mentioned previously, information security, to a large extent, relies on the security of the underlying infrastructure or network. The management direction, rules, regulations and procedures regarding the protection of information assets must be part of an information security policy. In order to change or influence the behaviours of people in an organization the information security policy and procedures must be properly communicated to all parties, such as employees of the organization and business partners (von Solms & von Solms, 2004). Employees of an organization would, of course, include IT staff. People could be the greatest threat to information security, and the related network security especially if policies, education, training and awareness are not properly utilized to prevent people from accidentally or intentionally posing risks to the security of network (Whitman & Mattord, 2011). Vulnerabilities may come from employees who do not comply with information security policies (Siponen, Mahmood, & Pahnila, 2014). Therefore, it is important that organizations like SANReN have policies in place in order to dictate the appropriate employee behaviour and better control what people can and cannot do on the network or network devices.

An investigation into the existing policies which manage the use of the SANReN network was conducted. The authors consulted appropriate people from SANReN concerning the current policies between SANReN and the SANReN beneficiary institutions. The authors were directed to the TENET website where the policies between SANReN and the beneficiary institutions were located. From the policies the authors were specifically looking for the operational roles and responsibilities of people in the SANReN network. The following questions were used to focus the content analysis of the TENET policies:

1. Who is allowed to have physical access to the SANReN devices of the beneficiary institutions?
2. Who can configure SANReN devices in the beneficiary institutions?

3. What minimum skills or qualifications should the people who configure SANReN devices in the beneficiary institutions have?
4. Are there training programs or some form of education that is given to the beneficiary institutions connected to the SANReN network?

The following policies were examined in order to determine whether human related issues regarding the previous questions have been addressed in the TENET policies. These policies were the only ones that existed on the website and according to the people of SANReN these policies are the only ones in existence that currently govern the use of the SANReN network: Acceptable Use Policy (AUP), Connection Policy and Privacy Policy. All these policies are created by TENET as it is the operating entity of the SANReN network. These policies are to the authors' knowledge the only ones that manage the use of the SANReN network. An analysis of these three policies was done in order to identify whether human factors are addressed in the policies and will be discussed in the following subsections.

### 5.1. Acceptable Use Policy (AUP)

The purpose of the TENET AUP is to outline for the SANREN beneficiary institutions the things allowed and not allowed on the network. It defines rules and responsibilities of the SANReN beneficiaries or participating institutions. According to the TENET AUP the beneficiary institutions are allowed to use the REN services for any legal activity which furthers the goals and aims of the institution, and only if their activity does not include any unacceptable uses. If the beneficiary institution does what is unacceptable on the network, the provision of the REN services may be discontinued by TENET. A few of the unacceptable uses of the REN services that are listed on TENET AUP are:

"Any attempt to use the REN services in a way that breaches or would breach the security of another user's account or that gains or would gain access to any other person's computer, software, or data or otherwise threaten another person's privacy, without the knowledge and consent of such person"

"Any failure to secure a server that is connected via the REN services to the Internet against being abused by third parties as an open relay or open proxy"

"Any effort to use the REN services in a way that circumvents or would circumvent the user authentication or security of any host, network account ("cracking or hacking")"

These are some of the unacceptable uses of the REN services which are listed in the TENET AUP. With regard to the questions posed previously, the TENET AUP stated nothing regarding physical access to SANReN devices in beneficiary institutions. Nothing was stated regarding people who are allowed to configure the SANReN devices. There was nothing stated about the level of skills or qualifications of people configuring SANReN devices in the beneficiary institutions and there was nothing mentioned regarding any form of training program which may be provided to beneficiary institutions by SANReN / TENET.

### 5.2. Connection Policy

The Connection Policy lists all types of connections which are available when connecting a Research and Education Network (REN). This policy specifies the differences, rules and responsibility of each connection. The REN network connection types are; direct on-site connection, direct PoP connection and indirect connection. The direct on-site connection is a type of connection which is under TENET operational management where the hand-off location is at the connecting site not the connecting party (beneficiary institutions). Hand-off location is the point where operational responsibility changes between the beneficiary institution and TENET (TENET, 2014). For the direct PoP connection the hand-off location is at the Point of Presence and TENET does not operate the terminating equipment at the connecting site and does not operate the access circuit between the connecting site and PoP. The institutions which have direct connection can then provide an indirect connection to other smaller research and education organizations around them. Places such as education and training colleges, schools and public museums can connect to the beneficiary institution's direct connection in order to access the REN services. However, the indirect connection is the responsibility of the SANReN beneficiary institution that connects it not of TENET. With regard to the questions previously posed, the TENET Connection Policy does not mention anything regarding physical access to SANReN devices in beneficiary institutions and nothing was mentioned about configuring devices. There was nothing stated about the level of skills or qualifications of people configuring SANReN devices in the beneficiary institutions and there was nothing mentioned regarding any form of training program which may be provided to beneficiary institutions by SANReN / TENET.

### 5.3. Privacy Policy

The TENET Privacy Policy explains how the personal information which TENET collects from TENETs contacts is used. TENET contacts are the people who work with TENET, such as the representatives of the beneficiary institutions, suppliers and other contractors (TENET, 2014). The TENET Privacy Policy states that TENET respects the privacy of its contacts and will protect the confidentiality of the contacts' personal information. With regard to the questions previously posed, the TENET Privacy Policy does not state anything regarding the physical access to SANReN devices in beneficiary institutions and nothing was mentioned regarding people who are allowed to configure devices. There was nothing stated regarding the level of skills or qualification of people configuring SANReN devices in the beneficiary institutions and there was nothing mentioned regarding any form of training program which may be provided to the beneficiary institutions by SANReN / TENET.

After conducting the analysis of the TENET policies, it can be noted that the AUP, Connection Policy and the Privacy Policy do not adequately address the human factors which might pose risks to the security of the SANReN network. None of the policies state the operational roles, responsibilities and procedures on the SANReN network. There was no documented framework that deals with security vulnerabilities posed by the human factors on the SANReN network and no clear guidelines and procedures concerning things like access control and authorisation. There was nothing mentioned about accessing the network devices nor about locking the doors or monitoring the room where these devices are placed. In other words, there were no direct rules and responsibilities or operational procedures addressed in these policies. If there are no proper procedures which people can abide by, the security of the network may be at risk. It may make it easier for unauthorized individual to gain access to the devices and, intentionally or unintentionally misconfigure network devices. Once an unauthorized person gains access to the devices even the technical solutions will not help in protecting the network. It is, therefore, very important that a security policy addressing operational concerns, for example, an operational security policy is put in place in the SANReN network and enforced in all the beneficiary institutions. Policies which outline the responsibilities and roles of people in the beneficiary institutions should be in place to better secure and manage the SANReN network. There is definitely a need for a formalized approach such as a framework or guidelines for addressing human related behaviour on the SANReN network.

## 6. Conclusion

This paper examined the existing policies which govern the use of the SANReN network. The TENET policies were examined to determine whether the issues of human factors, which could threaten the security of the SANReN network, were adequately addressed. The paper outlined that there were no current policies which address human factors on the SANReN network. Therefore a formalized approach to addressing human factors in the SANReN network is recommended as human factors could be the greatest risk to the security of the network. Just as there are formal policies in place to govern the use of technical controls, there should also be formalized policies in place to address human factors in order to strengthen the security of the SANReN network. Formal documents, such as an operational security policy, outlining the roles and the responsibilities of people involved in governing the SANReN network should be created and enforced in the SANReN beneficiary institutions. These policies should address all possible human related security concerns, ranging from Bring Your Own Device (BYOD) policies to security awareness and training. Future research would include creating a framework or guidelines which will address human factors in the SANReN network. The framework or guidelines could address issues such as the identification of role players and their responsibilities, determination of skills and the provision of a formalized training program to the beneficiary institutions.

## 7. References

Ashenden, D. (2008). Information Security management: A human challenge?, *13*(4), 195–201.

Ashton, K. (2009). That'Internet of Things'Thing. *RFID*. Retrieved from http://www.rfidjournal.com/articles/view?4986

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983–988. doi:10.1016/j.cose.2012.08.004

Grobler, M., & Bryk, H. (2010). Common Challenges Faced During the Establishment of a CSIRT. *IEEE*, 2–7.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists., *38*(2), 143–54.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, *28*(7), 509–520. doi:10.1016/j.cose.2009.04.006

Martin, D. (2012). *Tertiary Education and Research Network of South Africa NPC* (pp. 1–4). Retrieved from http://www.tenet.ac.za

Meraka Institute. (2007). African Advanced Institute for Information and Communication Technology. Retrieved from http://www.meraka.org.za/Faqs

Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception*. (C. Long, N. Stevenson, & J. Atkins, Eds.). Robert Ipsen.

Moller, K. (2007). Setting up a Grid-CERT : experiences of an academic CSIRT, *24*. doi:10.1108/10650740710834644

Mooi, R. (2012a). *Security Incident Response for the South African NREN* (p. 9). Retrieved from http://www.sanren.ac.za/wp-content/uploads/2012/11/IRT_background_survey_problem_SANReN.pdf

Mooi, R. (2012b). *Introduction to CSIRTs* (p. 5). Retrieved from http://www.sanren.ac.za/wp-content/uploads/2012/11/SANReN_CSIRT_Introduction.pdf

Mooi, R. (2013). *SA NREN CSIRC Model* (p. 14). Retrieved from http://www.sanren.ac.za/wp-content/uploads/2013/05/SA_NREN_CSIRC_Model-Published.pdf

Networking in South Africa.pdf. (n.d.).

PricewaterhouseCoopers. (2010). *Protecting your business*. *Veterinary Record* (Vol. 122). doi:10.1136/vr.122.17.421

Ritchey, R. W., & Ammann, P. (2000). Using Model Checking to Analyze Network Vulnerabilities. *IEEE*.

SANReN. (2012). *About SANReN* (pp. 1–11).

SANReN. (2014). SANReN Overview. Retrieved April 10, 2013, from http://www.sanren.ac.za/overview

Siponen, M., Mahmood, A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217–224. doi:10.1016/j.im.2013.08.006

TENET. (2014). TENET Standard Terms and Conditions. Retrieved January 22, 2014, from http://www.tenet.ac.za

TERENA. (2009). *TERENA COMPENDIUM*. Retrieved from www.terena.org/compendium

TERENA. (2010). Research and education networking FAQ. Retrieved from http://www.terena.org/activities/

TERENA. (2013). *TERENA COMPENDIUM*.

Thomson, K. L., & Von Solms, R. (2006). Towards an Information Security Competence Maturity Model. *Computer Fraud & Security*, 11–15.

UbuntuNet Alliance. (n.d.). TENET South Afrca. Retrieved from www.ubuntunet.net

UbuntuNet Alliance. (2013). *What is UbuntuNet?* Retrieved from www.ubuntunet.net

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective, *29*(4), 476–486.

Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers & Security*, *23*(4), 275–279. doi:10.1016/j.cose.2004.01.013

Whitman, M., & Mattord, H. (2011). *Principles of Information Security*.

Williams, P. A. H. (2008). In a “trusting” environment, everyone is responsible for information security, *13*(4), 207–215.

# APPENDIX B:
# VALIDATION INSTRUMENT

# The Validation of Guidelines for Addressing the Human Factor in the SANReN Network of Beneficiary Institutions

## 1. Introduction

The South African Research Network (SANReN) is a high-speed communication network designed primarily for research institutions, in order to provide South African research institutions and organizations with Internet access, as well as connecting them to research networks all over the world. This network is a part of the South African government's approach to cyber infrastructure in order to ensure the successful participation of SANReN beneficiary institutions in global knowledge. The SANReN beneficiary institutions are institution defined by the DST (Department of Science and Technology) as institutions allowed to be connected to the SANReN network. These beneficiary institutions are the current TENET institutions, such as the South African universities, research councils such as the CSIR, National Research Foundation (NRF), and various other research institutes. The roles and responsibilities of the SANReN network are distributed between the SANReN team and the Tertiary Education and Research Network of South Africa (TENET) team. The TENET team is responsible for operating the network and the SANReN team is responsible for building the backbone connectivity of the network.

The SANReN network, which is being rolled out across South Africa, has the potential to provide many opportunities and benefits to the people of South Africa. This network contributes immensely in the economic development of the country and projects of national importance, such as SKA, SALT, KAT7/MeerKAT, HartRaO/SAC for eVLBI experiments. One could view this network as one of the most important assets in the country. It is therefore; very important that the SANReN network is protected at all times in order to ensure the continued availability of the network.

## 2. SANReN Security

From a technical standpoint, network professionals who are knowledgeable regarding the SANReN network view this network as being adequately secure. Additionally, SANReN is in the process of establishing a SANReN/TENET CSIRT (Computer Security Incident Response Team) team that will be responsible for managing the security incidents of the SANReN network. However, technical controls should not be the only concern for addressing security on the SANReN network – human factors should also be of concern. The SANReN network may be vulnerable to risks posed by human factors even if technical controls exist on the network. Technical controls alone cannot necessarily guarantee protection of the network, as these technical controls still demand and depend on human beings for implementation and maintenance. Even if technical controls exist on the network, the SANReN network may be vulnerable to risks posed by human factors. There are humans involved in configuring the network devices, creating security policies or using the network as end-users. All the humans in an organization need to understand their roles and responsibilities in order to better protect the integrity, confidentiality and availability of information on the network. The people that the SANReN network connects and the people that configure the SANReN network devices may be the greatest vulnerability in the security of the network.

## 3. Research Problem

The problem that this research tries to address is; *the rolling out of the SANReN network has not formally considered the information security risks posed by the human factors on the networks of the beneficiary* *institutions.* The SANReN network's rollout strategy currently does not adequately address the human factors of information security. Therefore, the SANReN network may be vulnerable to risks posed by human factors, since human factors are normally the biggest threat to the security of a network.

## 4. Findings and Solution

In an effort to solving this problem, semi-structured interviews with the SANReN network engineers and a network engineer from one of the SANReN beneficiary institutions were conducted. The network engineer from the beneficiary institution (NMMU) was completely certain and confident about the technical and physical security of SANReN network. However, the network engineer also discussed a human factor related incident where, on one or two occasions, the SANReN/TENET network engineers managed to lock themselves out of the remote configuration session. They required local assistance from IT staff at the NMMU and the local IT staff had to make the configuration changes to the network device of SANReN. This is a human factor related incident, which could potentially compromise the security of the network. From this incident, it could be implied that even though the network might be seen as technically and physically secured, human factors could be the weakest link in the security of the SANReN network. What if a low-level skilled individual was asked to perform these changes on the SANReN network devices and ended up misconfiguring the devices creating more problems on the network? Having been granted access to the networking devices and, for example, knowingly or unknowingly connecting a device which contains viruses and worms which may be distributed throughout the network could have a severe impact on network security. The SANReN network may be exposed to security risks by allowing access to the wrong individuals because they are not aware of the skills or qualifications of the individuals.

Furthermore, a content analysis of SANReN/TENET policies that currently govern the use of the SANReN network was also conducted. The analysis of policies was conducted in order to identify whether or not human factors or human aspect issues that could threaten the security of the SANReN network were currently being addressed within SANReN/TENET policies. The following questions were used to focus the content analysis of the SANReN/TENET policies:

- Who is allowed to have physical access to the SANReN devices of the beneficiary institutions?
- Who can configure SANReN devices in the beneficiary institutions?
- What minimum skills or qualifications should the people who configure SANReN devices in the beneficiary institutions have?
- Are there training programs or some form of education that is given to the beneficiary institutions connected to the SANReN network?

It was discovered that the current policies governing the SANReN network do not adequately address the human factors. In those policies there was nothing  stated regarding people who are allowed to configure the SANReN devices, there was nothing stated regarding the level of skills or qualifications of people configuring SANReN devices in the beneficiary institutions and there was nothing mentioned regarding any form of training program which may be provided to beneficiary institutions by SANReN/TENET. There was no operational security policy, outlining the roles and the responsibilities of people involved in governing the SANReN network at the beneficiary institutions.

Furthermore, a literature review was conducted in order to determine what literature recommends for addressing the human factors in information and network security. Even with other SANReN documentation that has been closely looked at, none of those documents address the human factors on the SANReN network.

There is no documented framework or guidelines addressing security vulnerabilities posed by human factors on the SANReN network. Therefore, it is important that SANReN has policies and procedures in place in order to dictate the appropriate employee behaviour and better control what people can and cannot do on the network or network devices. Just as there are formal policies in place to govern the use of technical controls, there should also be formalized policies and procedures in place to address human factors in order to strengthen the security of the SANReN network.

This research, therefore, has proposed the following guidelines in order to address the human factors in the SANReN network of the beneficiary institutions. It is important to understand that guidelines number 1 and 2 could be seen as an ideal and could take a long time to be implemented. However, the other guidelines could be implemented in a short period of time, compared to employing people and cultivating an information security culture. It is also important to note that guideline number 3 can either be implemented as one program (SETA program) or can be implemented as an individual element of SETA as listed in guideline number 4, 5 and 6.

*Please respond to each guideline by indicating whether you strongly agree, agree, disagree or strongly disagree and provide some comments or suggestions regarding each guideline.*

**Suggested Guidelines:**

1. SANReN/TENET management should employ people at SANReN beneficiary institutions working specifically for SANReN/TENET.

   □ Strongly Agree □ Agree □ Disagree □ Strongly Disagree

   Comments and suggestions

2. SANReN/TENET should develop an information security culture to shape and influence the behaviour of IT staff at the beneficiary institutions.

   □ Strongly Agree □ Agree □ Disagree □ Strongly Disagree

   Comments and suggestions

3. SANReN/TENET should establish a security education, training and awareness (SETA) program for beneficiary institutions, in order to address human factors, such as human errors or failures, within the SANReN network.

   □ Strongly Agree □ Agree □ Disagree □ Strongly Disagree

   Comments and suggestions

4. SANReN/TENET should implement security awareness programs for beneficiary institutions to focus their attention on securing the SANReN network

□ Strongly Agree □ Agree □ Disagree □ Strongly Disagree

Comments and suggestions

5. SANReN/TENET should implement security training programs for beneficiary institutions in order to provide appropriate skills and knowledge for securing the network

□ Strongly Agree □ Agree □ Disagree □ Strongly Disagree

Comments and suggestions

6. SANReN/TENET should ensure that the IT staff at beneficiary institutions have appropriate qualifications, training, experience and certifications before granting access to SANReN devices

□ Strongly Agree □ Agree □ Disagree □ Strongly Disagree

Comments and suggestions

7. SANReN/TENET should develop security policies that address operational concerns within SANReN beneficiary institutions

□ Strongly Agree □ Agree □ Disagree □ Strongly Disagree

Comments and suggestions

8. SANReN/TENET should establish formal operational procedures specifying roles and responsibilities of IT staff at beneficiary institutions

□ Strongly Agree □ Agree □ Disagree □ Strongly Didagree

Comments and suggestions