A Model for Role-Based Security Education, Training and Awareness in the South African Healthcare Environment

Ophola Maseti

A Model for Role-Based Security Education, Training and Awareness in the South African Healthcare Environment

by

Ophola S. Maseti

Dissertation

submitted in fulfilment of the requirements for the degree

Magister Technologiae

in

Information Technology

at the

School of Information and Communication Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela Metropolitan University

Supervisor: Dr. Dalenca Pottas

January, 2008

Dedication

My sincerest gratitude and appreciation are extended to:

- The **Almighty** for giving me all the blessings;
- My Supervisor, **Doctor Dalenca Pottas**, You are a genius... Your input has ensured that this research is completed;
- My **Family** for allowing me to do what I wanted to do;
- My special **Friends** for believing in me and my other friends;
- Ms. **Bronwyn Kaplan** for all the time you spent proofreading this dissertation;
- Finally, the **Students** of NMMU for all your support.

"Our society is spoilt with choices today. Choices are presented to all of us. Some do good things, and by virtue of human nature, some do bad things. Never have I seen and felt that there is a greater need to protect individuals from being victims of privacy breaches than I have today." **– Ophola Maseti (2008) -**

DEPARTMENT OF ACADEMIC ADMINISTRATION
EXAMINATION SECTION – NORTH CAMPUS
PO Box 77000
Nelson Mandela Metropolitan University
Port Elizabeth 6013

Nelson Mandela Metropolitan University
for tomorrow

DECLARATION BY STUDENT

NAME: ..... Ophola Maseti .....

STUDENT NUMBER: 20116056 .....

QUALIFICATION: MAGISTER TECHNOLOGIAE: Information Technology .....

TITLE: A Model for Role-Based Security Education, Training and Awareness in the South African Healthcare Environment .....

DECLARATION:

In accordance with Rule G4.6.3, I hereby declare that the above-mentioned 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: 2007, January 11th .....

Table of Contents

List of Figures

List of Tables

Abstract

It is generally accepted that a business operates more efficiently when it is able to consolidate information from a variety of sources. This principle applies as much in the healthcare environment. Although limited in the South African context, the use of electronic systems to access information is advancing rapidly. Many aspects have to be considered in regards to such a high availability of information, for example, training people how to access and protect information, motivating them to use the systems and information extensively and effectively, ensuring adequate levels of security, confronting ethical issues and maintaining the availability of information at crucial times. This is especially true in the healthcare sector, where access to critical data is often vital. This data must be accessed by different kinds of people with different levels of access. However, accessibility often leads to vulnerabilities. The healthcare sector deals with very sensitive data. People's medical records need to be kept confidential; hence, security is very important. Information of a very sensitive nature is exposed to human intervention on various levels (e.g. nurses, administrative staff, general practitioners and specialists). In this scenario, it is important for each person to be aware of the requirements in terms of security and privacy, especially from a legal perspective.

Because of the large dependence on the human factor in maintaining information security, organisations must employ mechanisms that address this at the staff level. One such mechanism is information security education, training and awareness programmes. As the learner is the recipient of information in such a programme, it is increasingly important that it targets the audience that it is intended for. This will maximize the benefits achieved from such a programme. This can be achieved through following a role-based approach in the design and development of the SETA programme. This research therefore proposes a model for a role-based SETA programme, with the area of application being in the South African healthcare environment.

Chapter 1

Introduction

A brief overview of the dissertation as well as its main objectives is given in Chapter 1, providing background information on topics that will be discussed in the rest of the chapters, discussing key concepts and presenting the problem statement, objectives, research paradigm and the methodology of the research project. General security education, training and awareness principles and the security and privacy of patient healthcare information are also discussed.

"Imagine a time when the network is the world and the world is the network. A time when networked devices and mechanisms are so deeply embedded into daily lives that the only time they may ever be noticed is when they are not working." **– D. Crawford (2001) –**

"Information is the oxygen of the modern age. It seeps through the walls topped by barbed wire, it wafts across the electrified borders." **– Ronald Reagan -**

"I have a theory about the human mind. A brain is a lot like a computer. It will only take so many facts, and then it will go on overload and blow up." **– Erma Bombeck -**

"You lose your privacy, and sometimes, people don't see you as human." - **Shawn Wayans -**

1.1 Introduction

An investigation into the contemporary status of the South African healthcare sector will be conducted in this dissertation. The role that security and privacy plays in healthcare in terms of patient information is probed as well is as the legal liabilities thereof. The study then further investigates how information technology is transforming the way medical information is managed. It goes on to confirm that in order to protect this healthcare information, there is a need to find effective measures which safeguard it. In this research, the measure or control known as security education, training and awareness (SETA) will be investigated to this effect. The role of SETA programmes in helping employees to perform their security functions in the context of their jobs (or roles) is therefore

investigated. All these factors are considered in contributing towards proposing a role-based security, education, training and awareness model for the South African healthcare environment.

1.2 Background

Events where individuals have had their privacy rights breached are not new in the healthcare environment. This predicament is a perpetual issue as it is still apparent, even today. In a recent report released by the Government Accounting Office in the United States, it has been alleged that over 40% of federal health insurance contractors and medical aid agencies reported experiencing a privacy breach involving personal healthcare information over the past two years (Information Week, 2006). An astonishing statistic about these findings is the fact that these agencies and contractors collectively have access to medical data of more than 100 million people. Potentially, this breach of privacy can lead to a great deal of damage and badly impacts on victims whose confidential healthcare information has been compromised.

A classic example of this is that of the South African health minister's medical records that were leaked to a newspaper by someone who stole them from a private clinic. This caused much havoc, and the case ended up in court with the newspaper's editor facing a potential prison sentence. This example and others are further explored in Chapter 3.

Patients may become unhappy because of violations of their privacy rights; however, there are means to control these. Typically, patients are protected by various legislations ranging from country to country. In South Africa, there is a Constitution in place which ensures that each and every person has their right to privacy (University of the Witwatersrand, 2004). South Africa does not yet have its own legislation that deals with

information privacy, although a draft privacy bill is in the making. However, there are other acts that organisations have to comply with when it comes to dealing with patient information, which also touch upon the security and privacy of such information. Examples of these acts are the Promotion of Access to Information Act (PAIA), the South African National Health Act (SANHA) and the Electronic Communication and Transaction Act (ECT). This means that there is a legal liability towards ensuring that health information is protected, which is something that cannot be ignored.

The issue of the breach of security and privacy needs to be controlled before it becomes too rampant and results in devastating consequences for the healthcare sector. One of the ways to do this is by ensuring that healthcare personnel are well informed about methods of protecting patient information. Healthcare personnel also need to be taught about the legal liabilities that may arise should a patient's confidential medical information be disclosed without that patient's consent. These dynamics are even more complicated due to the fact that healthcare systems make use of technology which keeps changing all the time. Another problem that is brought about by IT systems is the issue of determining who, depending on their role, has access to what kind of information. Stenbakk and Oie (2004) state that when an employee is granted access to information, only the relevant information should be presented by the system. With all these technological changes, increased use of technology and access to healthcare information, healthcare organisations must ensure that their personnel stay informed, trained and educated about security-related issues in their working environment.

In order to ensure that the workforce is up to date about security issues, organizations will typically use SETA programmes. Such programmes can be more beneficial if they target the learners that attend, in a focused manner, ie if the programme is customized and a fit-for-all approach is not followed. With healthcare personnel fitting into various roles in their

organisations, it provides a way to address their security requirements according to the work that they do. A role-based SETA programme can be beneficial in this regard. This study will propose a model for security education, training and awareness which is focused along the lines of a role-based approach.

1.3 Key Concepts

1.3.1 The Healthcare Environment

The role of today's healthcare environment is to put patients at ease by providing them with familiarity and comfort (Healthcare Design, 2004). A healthcare environment is comprised of healthcare establishments, healthcare personnel and healthcare information systems. When all these elements are put together, they become a key driver for customer experience ("Healthcare Environment", n.d.).

In the following paragraphs, some of the key terms that are used in the healthcare environment will be explained. This is done to avoid confusion about the terms that will be used throughout this chapter and the rest of this dissertation.

Access: The ability to obtain, or the procedure to obtain data and information or resources for specific purposes and by specific users (Englebardt and Nelson, 2002).

Electronic Health Record: A set of information about patients and their treatment (Stenbakk and Oie, 2004).

Health Service Provider: Assesses records, maintains or improves a person's health; diagnoses, or treats a person's illness or disability; or dispenses, on prescription, a drug or medicinal preparation by a pharmacist (Office of the Federal Privacy Commissioner, 2002).

Healthcare Information System (HIS): The integration and presence of both hardware and software components that support the informatics to carry out all aspects of providing quality patient care and conducting the day-to-day business of healthcare (Englebardt and Nelson, 2002).

Individual: The person who is the subject of protected health information (University of California San Francisco, 2005).

Personal Information: Information or an opinion that identifies an individual, or allows their identity to be readily worked out from the information (A Guide to Privacy for Small Business, n.d.). It includes, for example, a person's name, address, financial information, marital status or billing details (Office of The Federal Privacy Commissioner, 2002).

Sensitive Information: A subset of personal information (A Guide to Privacy for Small Business, n.d.). It is information or an opinion about a person and includes (A Guide to Privacy for Small Business, n.d.):

- Racial or ethnic origin;
- Political opinions;
- Membership of a political association;
- Religious beliefs or affiliations;
- Philosophical beliefs;
- Membership of a professional or trade association;
- Membership of a trade union;
- Sexual preferences or practices; and
- Criminal record or health information about an individual.

Special rules apply to the handling of sensitive information (A Guide to Privacy for Small Business, n.d.).

Protected Health Information (PHI): Individually identifiable health information created or maintained by a covered entity, which relates to past, present, or future physical or mental conditions for provision of healthcare, and includes demographic information (Medical College of Georgia, n.d.). **PHI** is an individual's health information or data collected from an individual that is (University of California San Francisco, 2005):

- Created or received by a healthcare provider, plan or clearinghouse;
- Related to the past, present or future physical or mental health condition of an individual, the provision of healthcare to the individual, or the past, present or future payment for the provision of healthcare to the individual;
- Identifies or could reasonably identify the individual; and
- Is transmitted or maintained in electronic or any other form or medium.

Telemedicine: The use of telecommunications to provide consultations between providers and patients who are separated geographically (Englebardt and Nelson, 2002).

Information about ethnicity, religion and health is personal (A Guide to Privacy for Small Business, n.d.). Some of this personal information is extremely sensitive. As was previously mentioned, it must be noted that healthcare environments are the key drivers of patients' experiences. Good healthcare environments do matter greatly to visitors, patients, carers and staff ("Healthcare Environment", n.d.). It is crucial for role players in the healthcare environment to be aware, skilled and knowledgeable about ways of dealing with patient information. This, in turn, will ensure that patients and visitors are satisfied and that they will

consider returning to an establishment. Because health information is such a personal and sensitive matter, the next section of the study will discuss security and privacy in healthcare.

1.3.2 Privacy and Security Issues in the Healthcare Sector

Some of the long-standing needs and concerns in our society have been privacy, confidentiality, and security of personal health information, especially to healthcare providers and the public (Buckovich et al, 1999). Healthcare providers and organisations have a legitimate need to access information to deliver quality healthcare, which is important to the public. Since information technology has been accepted, beyond a doubt, as a way of living nowadays, the healthcare sector has had no choice but to integrate information technology into most of its systems. With this shift came the urgent need to balance privacy and access and to develop guiding principles, policies, and legislation to ensure that the public's information is protected safely from any unauthorised parties. With the use of information technology on the rise, access to sensitive and personal information has been easier for more individuals and entities.

Although the electronic medical record offers the promise of improved care and increased efficiency, introducing information technology into healthcare creates new risks to privacy, but also new means to protect privacy (The Privacy and Security Working Group, 2003). There are potential risks associated with automation and sharing of patients' medical records and a number of patients are well aware of these risks. Patients can withhold sensitive information from their clinicians that could be vital to their care, as a result of concerns about privacy and security. Consequently, the value of a patient's medical records to other clinicians treating the patient, researchers and public healthcare officials, can be reduced.

One of the most important acts for an organisation in the modern era is to sensitize, train and educate its employees on the value that the organisation places on the security and privacy of its customers' or patients' information, as well as how to implement security and privacy protection of healthcare information. This is normally achieved through the running of a SETA programme.

1.3.3 General SETA Principles

The purpose of security education, training and awareness (SETA) is to (NIST 800-50, 2003):

- Enhance security by improving awareness of the need to protect system resources;
- Develop skills and knowledge so computer users can perform their jobs more securely; and
- Build in-depth knowledge, as needed, to design, implement, or operate security programmes for organizations and systems.

When a SETA programme is envisaged, it must be known who is going to be targeted with the programme and what they should be taught. This will ensure that there is sufficient return-on-investment (ROI) on the resources spent to bring the programme to fruition.

The NIST 800-16 (1998) states that the learning of a security education programme is a continuum. It starts with awareness, constructs to training and then develops into education.

The three levels of the learning continuum can be explained as follows:

Awareness: As the learner is only the recipient of information and does not actively participate (NIST 800-16, 1998), the purpose of an awareness programme is to stimulate and motivate those being trained to care about

security and to remind them of important security practices (NIST 800-50, 2003).

Training: Training focuses on providing the knowledge, skills, and abilities specific to an individual's role and responsibilities relative to IT systems (Federal Agency Security Practices, 2000).

Education: The education level of the learning continuum integrates all of the security skills and competencies of the various functional specialities into a common body of knowledge.

Each person has a responsibility to every other person. All IT services are at risk when an incident happens. It is of importance that all the role-players in an organisation are aware of, trained and educated about the significance attached to security and privacy. To this effect, generally accepted principles and best practices in SETA will be applied in this research to propose a way to ensure that healthcare practitioners obey their responsibility towards the security and privacy of patient information.

1.4 Problem Statement

With South Africa being a relatively new democracy, many issues that relate to personal privacy have not been addressed adequately by healthcare organisations as well as the national government. National and international research shows that there is significant concern about the lack of privacy protection for South African citizens' medical records and health information (Council for Medical Schemes, 2002).

The main problem addressed in this research is the fact that healthcare practitioners in South Africa are potentially not aware of, skilled and educated in security and privacy issues with regard to patient healthcare information. In order to address this problem, the following issues must be investigated:

- What are the strategic imperatives of the South African National Department of Health and how is the healthcare sector made up in terms of resources and expenditure?
- Has there been an increase in technology adoption in the South African health sector to the extent that it is contributing to the effective interpretation and dissemination of health information?
- What are the requirements for the security and privacy of patient healthcare information and is there a legal liability?
- How can education, training and awareness be used to effectively solve the problem of a lack of awareness, skills and knowledge in maintaining the security and privacy of health information?

Addressing the afore-mentioned research questions will ensure that the objectives discussed in the following section, are achieved in this dissertation.

1.5 Objectives

The major objective of this study is to propose a role-based SETA model for the South African healthcare environment. The model provides South African healthcare organisations with an approach to use when it comes to educating healthcare personnel about security and privacy aspects that come into play when dealing with patient information. The model further promotes a targeted approach rather than “one-size-fits-all” to ensure that the SETA programme is beneficial considering the resources that are required to implement such a programme.

The following sub-objectives will be attended to, in order to support the main objective of this study:

- Investigate the current state of the South African healthcare sector;

- Identify the requirements for and legal obligation to the security and privacy of patient healthcare information;
- Discuss SETA best practices and generally accepted principles; and
- Through logical argumentation, propose a role-based SETA model for the South African healthcare environment.

In order to achieve these objectives, the following research methodology will be applied.

1.6 Methodology

The research conducted for this project, is primarily of a phenomenological nature. This is also known as interpretivist research - the researchers gather information and filter it, while involving themselves in the study. In this kind of research, subjectivity plays a role, with the researchers having to argue towards the interpretation of the research area and the proposed solution.

Since the research is predominantly of a phenomenological nature, the execution of a proper literature study was employed as a suitable research method. An extensive literature study thus forms the basis of the research. An extensive literature study was conducted to gather information as pertaining to the following:

- The reform of the South African healthcare sector;
- The security and privacy of patient healthcare information; and
- Principles and best practices of security education, training and awareness.

With a clear understanding of the requirements for security and privacy having been identified, arguments were employed that attest to the fact that in order for the awareness, skills and knowledge amongst healthcare personnel about the importance of protecting the privacy and security of patients' healthcare information to be improved, a SETA programme is essential.

The information derived from the extensive literature assessment and arguments were then considered in contributing towards a model to implement a role-based SETA programme in an organisation in the South African healthcare environment. Such a programme will, in turn, improve the way healthcare personnel perform their security-related functions.

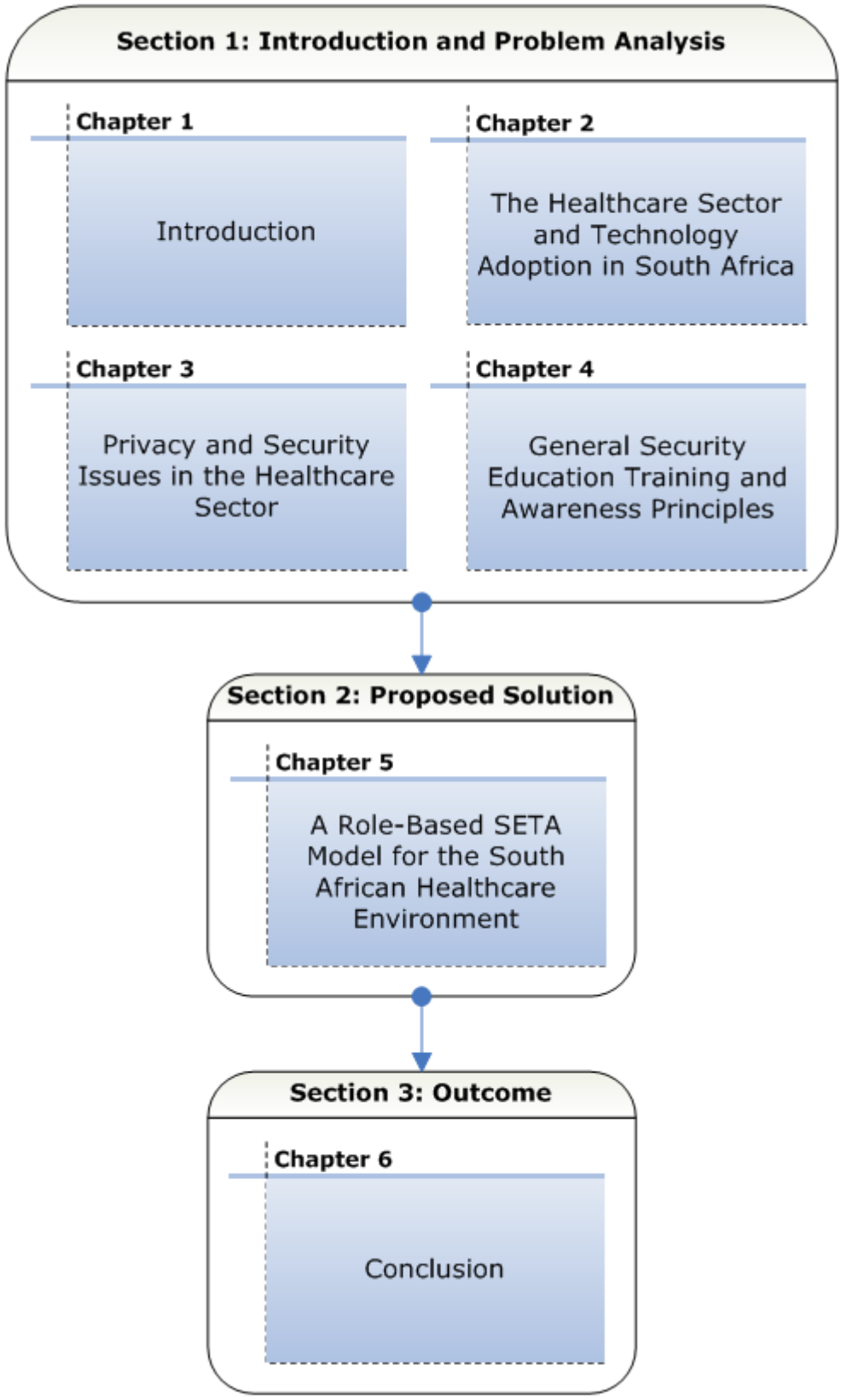
1.7 Structure and Layout of Dissertation

The layout of the dissertation is divided into three sections and six chapters and is depicted in Figure 1.1.

Section 1 is comprised by the first four chapters of the dissertation and covers the background of the research area. Chapter 1 provides a brief introduction to the dissertation and expounds the problem statement, objectives and methodology of the research. Chapter 2 discusses the transformation of the South African healthcare sector. In addition to this, it is discusses to which extent technology has been adopted and what is being done to improve quality assurance in this particular sector. In Chapter 3, a discussion of the privacy and security issues that pertain to patient information in the healthcare sector is provided. The legal liabilities that are involved when dealing with this information are also analysed. In Chapter 4, generally accepted SETA principles and best practices are outlined first. The chapter further discusses how a SETA programme can be implemented and how an organisation can evaluate its effectiveness after it has been implemented.

Section 2 provides the solution for this dissertation by proposing a role-based SETA model to be implemented in organisations in the South African healthcare environment. This is done in Chapter 5.

Figure 1.1: Layout of the Dissertation



Section 3, Chapter 6 presents the conclusion of the dissertation. It is shown that the objectives of the research as specified in Chapter 1, have been reached. Based on the outcomes of this dissertation, the chapter further recommends future and continued research.

1.8 Conclusion

This chapter took care of the formalities of writing a dissertation, by introducing the research area and then narrowing down to the problem statement as identified in the research area. It goes further to indicate what the proposed solution to the problem statement is, by looking at the main and sub-objectives of the research. In the next chapter the groundwork is further expanded by reporting on the literature study conducted about the South African healthcare sector.

Chapter 2

The Healthcare Sector and Technology Adoption in South Africa

This chapter takes a look at the healthcare sector in South Africa. The sections start by investigating what the government is doing to improve this particular sector. There is also a brief discussion on the differences in services offered by private and public healthcare institutions. Technology adoption is also touched upon.

"*In a developing country like ours, we have too many other health concerns to warrant healthcare budgetary expense on such a device. TB, HIV, infant mortality and cost of health services to the general public all take priority on already scarce financial resources, and our hospitals are overcrowded. You cannot spend money on a nice-to-have while you do not have beds for patients or doctors to service the patients."* **– Unnamed Doctor (2005) -**

"The leveraging of information and communication technology (ICT) to connect provider and patients and governments; to educate and inform healthcare professionals, managers and consumers; to stimulate innovation in care delivery and health system management; and, to improve the healthcare system." – **SAITIS (2002)** -

2.1 Introduction

South African society - like many other developing societies - is pre-eminently a society in transition, and this is reflected in its disease and death profiles (Bradshaw and Buthelelzi, 1996). The authors claim further that South Africa has been going through a profound social and political change for the past number of years since democracy started. The Bill of Rights in the Constitution gives everyone in South Africa the right to have access to a whole range of socio-economic rights including housing, healthcare, food, water, social security and education ("Towards Greater Equity", 2004). The Constitutional Court has further interpreted this as placing a legal obligation on the government of South Africa to ensure the progressive realization of these rights. With health being the emphasis of this study, the author believes that it is imperative for the Ministry of Health to be an effective steward to oversee the operations of the

healthcare sector. These operations should ensure that the citizens of South Africa have access to a national health system that is going to provide a good service and that is going to be fair to all. This fairness must be accomplished regardless of whether it occurs in the public or private health sectors.

As new technologies are developed and deployed, it is paramount that both the business and public health communities understand the dynamic relationships evolving between the development of a particular technology and health (Mechael, 2002). Governments have realised the need to develop standards and infrastructure to allow for more effective use of information technology to promote higher quality care and to reduce healthcare costs ("Secretary Thompson", 2004). Developing countries frequently make use of health-information systems and telemedicine amongst a whole lot of other ICT applications (Mechael 2002). The case is the same with South Africa; however, in South Africa, the rate of technology is not as swift as it should be because of various factors that the government is still faced with, for example, poverty. There are many advantageous ways in which ICT can be and is being integrated into communities in poor countries that are having an impact on health (Mechael 2002). Information technology in healthcare can improve the quality of care, reduce medical errors and lower administrative costs at the same time; security and privacy of electronic medical records would be improved over the protection of paper-based records ("Thompson Launches", 2004).

In the next few sections, this study will take a look at what is being done to reform the national healthcare sector after all the injustice during the years of apartheid. The study will then look at technology adoption here in South Africa.

2.2 Reform of the South African Healthcare Sector

South Africa has had an unfortunate event, apartheid, in its past. Back then, there were too many policies of the apartheid government that did not allow all South Africans access to proper healthcare. Now that South Africa is a free and democratic country, all the damage from the past needs to be repaired by the government. All legislation, organisations and institutions related to health have to be reviewed with the purpose of the complete transformation of the national healthcare delivery system (ANC, 1994a).

2.2.1 Strategic Priorities of the Department of Health

In May 1994, a week after the inauguration of President Mandela, the African National Congress (ANC) published "A National Health Plan for South Africa" ("Towards Greater Equity", 2004). This book contained strategies that would guide and form the shape of the South African healthcare sector in years to come.

"When we started the term of office of this government in 2004, we set ourselves a series of goals which we sought to achieve when this term ends in 2009. These goals are contained in a document which we called Strategic Priorities for the Health Sector: 2004-2009 (popularly called the 10-Point Plan)" (Department of Health, 2006). The 10-Point Plan clearly shows that the government is aware that the healthcare sector needs to effect serious changes in order to benefit all South Africans. Below follows a brief summary of the department's key priorities and activities contained in the 10-Point Plan.

Priority 1: Improving governance and management of the national health system. This includes the strengthening of communication, corporate

identity, management of structures and governance. Adopting the Health Industry Charter and marketing of health policies and programmes are also touched upon.

Priority 2: Developing strategies to promote healthy lifestyles and to reduce chronic diseases caused by unhealthy lifestyles.

Priority 3: Contributing towards human dignity by improving quality of care. Strengthen the hospital accreditation system and community participation as well as improving the clinical management of care at all levels.

Priority 4: Improving the management of communicable diseases and non-communicable illnesses. The order of the day here is the improvement in immunisation coverage and in the health management of all children under the age of five.

Priority 5: Strengthening primary healthcare, Emergency Medical Services (EMS) and hospital delivery systems. Strengthening both hospital services and mental health care as well as implementing provincial EMS plans are considered the key activities under this priority.

Priority 6: Strengthening support services. The National Health Laboratory Service services shall be strengthened, a forensic service shall be developed and a health technology management system shall be implemented. Other activities vary from establishing an integrated disease surveillance system to ensuring that medicines are of quality, are safe, effective and affordable.

Priority 7: Human resources planning, development and management. This section deals with implementing the national human resource plan and strengthening human resource management.

Priority 8: Strengthening the health system's planning, budgeting, monitoring and evaluation, strengthening the use of the health information system and obtaining Cabinet approval for a Social Health Insurance policy.

Priority 9: Preparing and implementing legislation. A priority of note, this deals with implementing the following: a) The Mental Health Care Act, b) The National Health Act, c) The Provincial Health Acts, and d) The Traditional Healers, Nursing and Risk Equalisation Fund Bills.

Priority 10: Strengthening international relations focusing on strengthening the implementation of the NEPAD strategy and SADC. Donor coordination and the implementation of bi- and multi-lateral agreements will also be strengthened**.**

The afore-mentioned priorities relate to this research in terms of the use of health information systems (Priority 8) and the preparation and implementation of legislation (Priority 9). The South African National Health Act, which inter alia deals with the protection of health information, is relevant. This act (and others) are discussed further in Chapter 3, Section 3.5, which deals with legal liability in the protection of healthcare information.

The Department, as is reflected in the Plan, will improve the health facilities and the quality of care that is provided in these facilities, including clinics and hospitals. In this regard it planned to (and did) introduce a hospital improvement plan in April 2006. With respect to healthcare programmes, two programmes addressing TB and HIV respectively, were prioritised in line with the decisions taken by World Health Organization, Regional Office for Africa (WHO/AFRO). In 2006, a TB Crisis Plan was launched to deal more decisively with the burden of the

disease as well as an Accelerated HIV Prevention Plan (Department of Health, 2006).

The National Health Plan has been guiding the healthcare sector and is still relevant today. Almost everything that the National Department of Health has done is in there, and it intends to continue with the unfinished business ("Towards Greater Equity", 2004). It is important that the government must have some means to measure its achievements against its goals. In order to know the progress in terms of achieving goals, it is imperative that it reflects on what it has been able to achieve thus far. In 2005 a report, the "South African Health Review" was produced to this effect (Ijumba and Barron, 2005).

Much has been achieved in terms of the reform of the healthcare sector, although as much remains to be done, as confirmed in the following statement: "These priorities are based on an assessment of what we have achieved in the past 10 years and what work remains to truly transform the health system to better meet the needs of all those who live in South Africa. Whilst we are justifiably proud of our achievements we need, in the next five years to work hard with our partners to strengthen the health system so that we can provide accessible, good quality health services to all" (Department of Health, 2006). The government is willing to compromise and collaborate closely with its partners and bring fresh ideas that would ensure that the health system of South Africa is strengthened. This is good news for the South African public, as the government has had problems with ensuring that delivery in the Department of Health is of good quality.

2.2.2 The National Policy on Quality in Healthcare

The aim of the Department of Health is to promote the health of all people in South Africa through a caring and effective national health system based on the primary healthcare approach (Department of Health, 2006). Furthermore, based on the strategic priorities document, the Department of Health provides stewardship to the national health system through policy formulation, development of legislation, providing technical support to provinces, setting of norms and standards and monitoring inter-provincial equity.

The present time calls for the public healthcare system to be in dire need of refocusing its collective efforts towards improving the quality of care provided in public health facilities and communities (National Department of Health, 2007). The Department of Health adopted a National Policy on Quality in 2001 (Department of Health, 2006). The main objective of this policy is to provide a way to improve the quality of care in both the public and private sectors (National Department of Health, 2007). The national aims for improvement include, but are not limited to (National Department of Health, 2007):

- Addressing access to healthcare;
- Increasing patients' participation and the dignity afforded to them;
- Reducing underlying causes of illness, injury, and disability through preventive and health promotion activities;
- Expanding research on evidence of effectiveness;
- Ensuring the appropriate use of healthcare services; and
- Reducing healthcare errors (adverse events).

Based on the national policy, all the provinces should have established provincial policies and quality assurance units to lead and co-ordinate efforts on quality improvement. There should also be complaints systems and procedures in place for all the provinces and the national department.

To support this notion even more, the government has to ensure that there is proper infrastructure and resources throughout the whole country. This can be done by investing and spending money wisely in the healthcare sector. Achieving the goal of a quality healthcare system requires a national commitment to measure, improve and maintain high-quality healthcare for all its citizens (National Department of Health, 2007). This further involves measuring the gap between standards and actual practice, and working out ways to close the gap.

It is important to note that "measurement" is key in achieving quality. This suggests that proper health information systems should be in place, to facilitate the availability of the data necessary to make these measurements. At the same time, the importance of protecting such information comes to mind. This will be further discussed in Chapter 3, which addresses privacy and security issues in the healthcare sector.

2.2.3 Expenditure

In 1994, South Africa was spending R550 per person per year on healthcare, which was only 5% of the GDP (ANC, 1994b). However, the percentage of GDP spent on healthcare services rose to 8.6 by 2004 (WHO, 2007). This is more than the 5% that the World Bank estimates should be appropriate to provide basic healthcare for all in developing countries like South Africa.

Table 2-1, below, provides the total expenditure on health as a percentage of gross domestic product, by the South African healthcare sector over the last number of years.

Table 2-1: Total Expenditure on Health as % of GDP. Source (HST (2007a); WHO (2007))

Year	% of GDP Expenditure
2000	8.1
2001	8.4
2002	8.3
2003	8.5
2004	8.6
2005	8.1

From the above statistics, it can be deduced that South Africa has been ensuring that healthcare is taken care of (from a budgetary perspective). Considering the sizeable investment in healthcare, the South African healthcare sector should be striving to be included along the same lines as those of upper middle-income countries. In order to ensure that the South African healthcare sector does really reach its true potential with regards to reformation, there must be an even distribution of resources, proper planning and there should be no corruption. It is the lack of coordinated planning, the mismanagement of resources and the inefficiencies in both the public and the private sectors that result in South Africans getting, at the moment, so little value for their money (ANC, 1994b).

2.2.4 Implementation of Strategies

The state is the largest social institution; therefore, its capital, human resources, managerial, technological and organisational requirements must be expected to reflect the society from which it originates (Mbeki, 2005). The government is surely paying attention to the reformation of the healthcare sector in South Africa and has a good plan, from a strategic level point of view, but the implementation of the strategy at the operational level has not been successful because of certain factors. Amongst these factors, but not limited to them, are shortages of staff members and inappropriate infrastructure.

The Minister of Health, Dr Manto Tshabala-Msimang made a 10-year democracy celebration speech in Durban in 2004 entitled “Towards Greater Equity in Health Care” (“Towards Greater Equity”, 2004). The Minister felt that the major strides that have been taken towards implementing healthcare strategies and ensuring greater equity in health needed to be celebrated. The Minister referred to the following as being attained so far:

- Political equality;
- A Constitution with a Bill of Rights;
- Significant progress towards gender equity; and
- Restoring the dignity of people living with disabilities.

The Minister claimed that these achievements have a direct impact on the health of the South African people. She went on by saying that the healthcare sector has done its bit in the whole process of transformation towards greater equity. The Minister further claimed that there is still great inequity and that there are still many challenges to be addressed, as many South Africans still lacked jobs and the dignity that go with them. Nevertheless, she was still proud of what had been achieved so far.

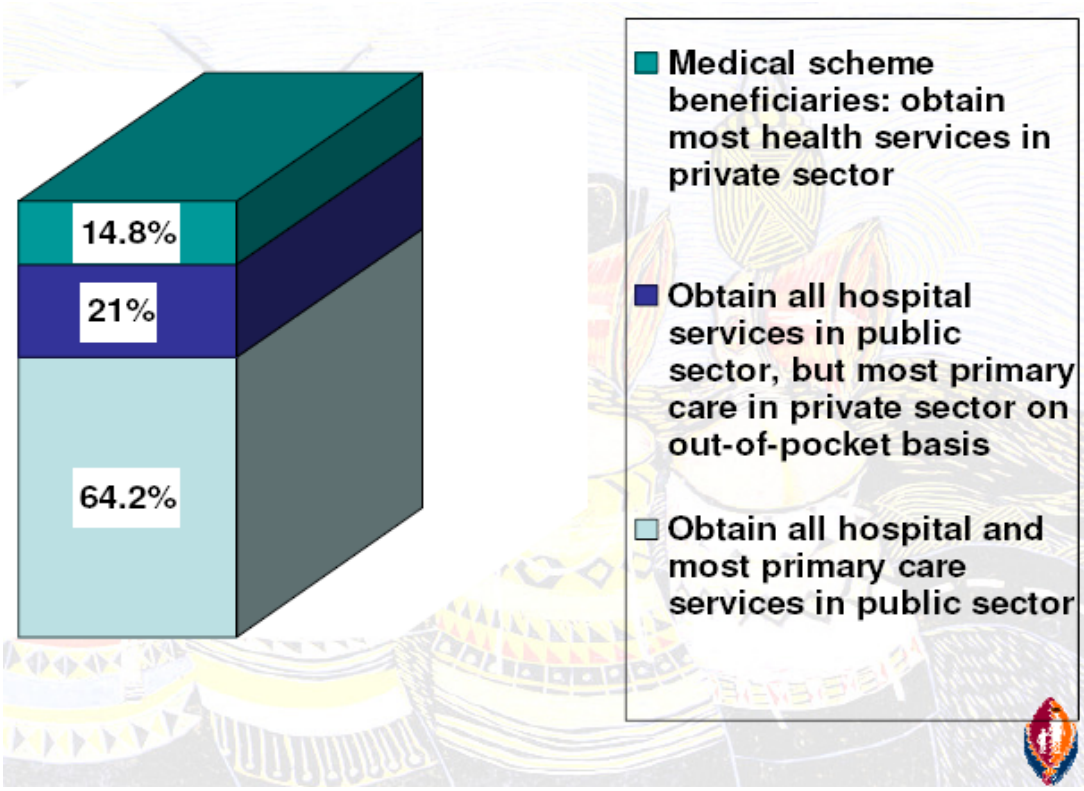
Usually organisations have excellent strategies, but the mistake that they make is not communicating these strategies to the people that generate the value of the organisations (National Department of Health, 2005). The strategic planning newsletter document by the National Department of Health (2005) says that if this can be applied to the Department of Health, it will mean that the front-line workers and managers should be engaged in the development of these plans, and the strategy of the Department of Health should be communicated to those that will assist in achieving the strategy. However, these actions seem to be effortless in theory but they emerge to be rocket science in practice. With the strategies involving technology and the healthcare sector involving a great many people, there must be a way to distinguish that whenever there is a new strategy, the front-line workers are included as part of that strategy. This will be crucial

for the healthcare sector in South Africa, to truly achieve its aims towards reformation.

2.3 The Alley between the Private and the Public Healthcare Sectors

Harrison et al (2007) state that South Africa has a large, well-developed, resource-intensive and highly specialised, formal, private healthcare sector. This sector is primarily funded through contributions to medical schemes, which provide healthcare insurance coverage to some 7 million beneficiaries (of a total South African population of approximately 47 million) (Harrison et al, 2007). Figure 2-1 illustrates this scenario.

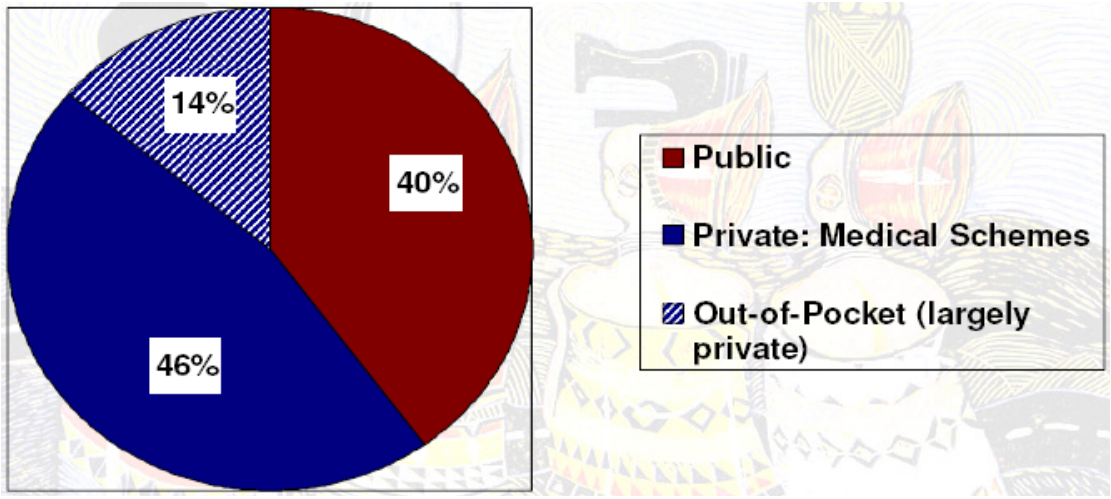
Figure 2-1: Estimated % of SA Population by Healthcare Sector. Source Harrison (2007)



Each year, 8% or more of the gross national product (GNP is an indicator of the wealth produced by the country) is spent on the national health system, including both the public and private healthcare sectors (National Department of Health, 2006). Below is a breakdown of the expenditure and the number of people affected by the two sectors, as can also be seen in Figure 2-2 (National Department of Health, 2006):

- On average, 60% of this is spent in the private sector, which provides care to 20% of the population;
- 80% of the population relies on the public healthcare system for healthcare; this sector receives 40% of total expenditure on health.

Figure 2-2: Health Expenditure in SA. Source Harrison (2007)



The inequities in the healthcare system, particularly between the public and the private healthcare sectors should be a concern for all stakeholders (Opening Address", 2007). Beresford (2007) does claim that only around 44% of healthcare spending goes through the public sector. The rest goes through the private sector; yet, only about a fifth of the population has regular access to private healthcare (Beresford, 2007). The Minister of Health has expressed concerns about the slow pace of transformation of the private healthcare sector, along with ("Opening Address", 2007):

- Issues of cost escalations;
- Lack of transparency in pricing; and
- This particular sector's contribution to inequities.

According to the "Opening Address" (2007), the Minister states that legislative changes and other means available should be used to ensure that the private healthcare industry will genuinely contribute to the realisation of the right of access to healthcare as enshrined in the South African Constitution. In exercising the constitutional requirement to take legislative and other measures to achieve the progressive realisation of the right to healthcare, the healthcare sector cannot be left to operate on its own: there needs to be an intervention by relevant stakeholders for these particular reasons (Harrison et al, 2007):

- Firstly, in the healthcare market, forces tend not to give rise to an optimally efficient and competitive market. This is evident, for example, in the rapid consolidation of the private hospital market over the past decade into the hands of three major market players, which have little need to engage in price competition and, instead, compete largely for the allegiance of doctors. The creation of an oligopoly in the private hospital market is, in all likelihood, a major contributor to healthcare-cost escalation in the private sector.
- Secondly, in the private healthcare market, the uncontrolled development of this sector has had a negative impact on resources in the public sector. The most important example of this is the massive migration of health personnel from the public sector to the private healthcare sector, resulting in critical human-resource shortages in the public sector. The answer to this does not necessarily lie simply in restrictions on professional practice, but it provides a basis for approaching the issue of supply and distribution of human resources between public and private sectors in an integrated and coordinated fashion.
- The third reason for intervention is that if cost trends in the private health sector continue to be unchecked, the private sector is unlikely to be sustainable in the future. Already, the proportion of the population who are covered by medical schemes is diminishing, resulting in a growing proportion of the population which is reliant on the relatively under-resourced public sector. For the private sector to play a valuable role in the development of the South

African health system, it should be lessening the burden on the public sector rather than adding to it.

- Perhaps the most important reason why the private sector cannot be left to an unregulated market is that it is intolerable, from a public policy perspective, that the socio-economic status of an individual is a primary determinant of the level of access to healthcare that the individual can receive. The hugely skewed distribution of healthcare resources between persons dependent on public and private sectors is inequitable and has no place in a society trying to shake off the remnants of a history of social injustice.

The Minister of Health has confessed to realising that there are several challenges that need to be met in the Department of Health's quest to truly transform the healthcare sector (Department of Health, 2006). The Minister stated one of these as the need to achieve an improved partnership between the private and public healthcare sectors. In addition, the Minister believes that the private healthcare sector urgently requires a coherent regulatory framework to ensure that it operates in the best interests of all the citizens of the country and not just its shareholders ("Opening Address", 2007).

The Department of Health is well on its way to drafting a Health Charter by exploring how to pool resources available to the healthcare sector, so that every South African can have access to a caring and high quality health system that is affordable (Department of Health, 2006). The public and private healthcare sectors need to find a common ground for the sake of all South Africans. As South Africa is still a developing country being governed by a new democracy, these two sectors need to commit towards providing fair and better healthcare for the whole populace.

What is required now is a clear road-map to be developed by government, in consultation with all relevant stakeholders, in terms of how it sees the ongoing development of the health system in a manner which harnesses

the resources of both public and private sectors to the equitable benefit of all South Africans (Harrison et al, 2007). Any national policy must, therefore, recommend ways to come up with solutions on serious issues that concern both the private and public sectors, and by so doing contribute towards strengthening the partnership between the public and private sector to the benefit of all South Africans (National Department of Health, 2006). The achievement of equity and social solidarity in access to healthcare is a fundamental imperative of the right of access to healthcare (Harrison et al, 2007).

Having discussed the South African healthcare milieu in terms of its strategic and quality priorities, its expenditure patterns, problems with implementation strategies and lastly the public and private sectors, it is now relevant to consider to which extent information technology adoption has progressed in South Africa.

2.4 Technology Adoption in South Africa

Calle Hedberg, who is a researcher and systems designer at the South African Health Information Systems Programme, alleges that 90 to 95% is spent on advanced Hospital Information Systems in larger hospitals Hedberg (2003). The author deduces that Government expenditure on Healthcare Information Systems has not changed in line with the shift towards the Primary Healthcare approach, which is believed to be why the South African healthcare sector has a slow improvement in technology.

Health is knowledge-based, whether considered in relation to the delivery of health services by health professionals, or in public health terms as the result of individual, family and community decisions about the way people live and behave (Mechael, 2002). Thus, health is profoundly affected by the application of Information and Communication Technology (ICT), which has changed the way people can access knowledge and the way they communicate with one another in daily behaviour (Murray and Dopson, 2002). Health information technology yields huge savings as it

has the potential to greatly improve healthcare (United States Department of Health and Human Services, 2004). It can also offer much greater access to and control of health records by consumers themselves ("Thompson Launches", 2004). Since the future of healthcare delivery institutions lies in cost-effective healthcare, healthcare delivery institutions will need and use information technology to meet their client demands and stay competitive (Institute of Health Systems, n.d.). Furthermore, the Institute of Health Systems (n.d.) states that general-purpose information-technology solutions are usually insufficient for the special needs of the healthcare sector.

The South African government is undergoing a process of enhancing the South African healthcare sector as mandated by the Constitution of South Africa and the Bill of Rights. This process has to involve information technology – in fact it is a critical success factor in this process.

As information and communication technologies are rapidly changing the way individuals live, firms do business, governments administer and nations interact, it is clear that no country will be left untouched by the information revolution (Hodge and Miller, 1997). Member states of the World Health Organisation (WHO) must have established "structures and processes to ensure continued improvement of the quality of health services and an appropriate development and utilization of technology" (Health Technology Assessment, n.d.). This subject is addressed in Goal 31 of the World Health Organisation's "Health for All" strategy. So it is evident that the focus on the regulation and management of Health Technology is not a South African trend alone.

Both the European Union (EU) and globally (the G-8) have recognised healthcare as one of the sectors in society with great potential for ICT and with great benefits to be gained through their application in the Information Society (South African Information Technology Industry Strategy, 2002). The South African Information Technology Industry

Strategy (2002) further states that governments must be encouraged and, in particular health ministries, to facilitate the implementation of what is commonly called “e-health”. With the implementation of “e-health” being emphasised in most developing countries all over the world, South Africa has accelerated the concept of a District Health Information System.

The District Health Information System has been implemented in all South African provinces; however, the effective use of this data has been minimal. An assessment of various hospitals in the Eastern Cape during 1999 indicated that (Shaw, 2002):

- Data is collected ‘at all levels in hospitals, but most of it is never used’;
- Indicators are submitted to the district offices, but give a ‘very bland picture of administrative activities, and no feeling of what goes on inside hospitals’.
- ‘Registers are non-standardized, and tend to be anarchic, and hand-written’, and often on an assortment of different types of paper and books.
- ‘Analysis of data is minimal at all levels’.

If the implementation of the District Health Information System is to be successful, the data collected must be analysed thoroughly and used extensively whenever there is a need to do so. There seems to be a lack of integration between the hospitals and district management, which is hampering the government in its efforts to improve the services offered by the healthcare sector (Hedberg, 2003). Hedberg (2003) professes that there have been persistent problems with data quality, but data flows and utilisation of data/information have been a major achievement and largely a unifying force across the country. Data usage problems might be decreased if district managers work together with hospital managers by having meetings, possibly quarterly, to discuss the data that has been generated for the past three months and taking decisions thereafter that

are going to benefit the public making use of the health services. By doing so, they would be ensuring that the utilisation of healthcare data is enhanced.

In a report by Asia and Pillay (2003) it is stated that in terms of data capture and use, most health districts in the country are still at Level 1 (data is being captured but its quality and use requires major improvement), whereas Level 3 (data of good quality collected and used for service improvements) is the target for all health districts. The authors further say that to reach this target in all health districts, it is important that provincial, local government and district information officers work with clinic supervisors and clinic managers.

Available information indicates that in South Africa, there is a growing demand for improved ICT in the healthcare sector (South African Information Technology Industry Strategy, 2002). At present, there are various ongoing projects that have been initiated by the South African government that address technology adoption within the healthcare sector.

The Health Systems Trust (HST) is an independent organisation that was formed in 1992. Its core activities are health-systems research, health-systems development and information dissemination. The HST aims to support transformation towards a more equitable provision for healthcare services, especially to meet the needs of the most disadvantaged. The HST has a sound working relationship with the Department of Health and a full explanation of the technologically-oriented projects funded by the government can be found on their website www.hst.org.za. Below is a list of some of the projects (HST, 2007b):

1. The National Health Information Systems project [April 2005 – Present]: This project aims to provide technical assistance and support to the national and provincial departments of health to strengthen the use of

health and management information systems, with a focus on the District Health Information System (DHIS);

2. Mpumalanga Monitoring and Evaluation project [August 2007 – October 2007]: The aim of the project was to strengthen healthcare service delivery in Mpumalanga Province by developing an effective system for ongoing monitoring and periodic evaluation of health programme implementation;

3. The Emergency Medical Services (EMS) Health Information Systems project [November 2006 – May 2007]: the aim of the project was to ensure optimal availability of EMS data, ensuring data quality, ensuring optimal flow of data and training of EMS managers on utilisation of data;

4. The Data Manager (National Department of Health Primary Healthcare, Districts and Development) project [June 2006 – May 2007]: This project incorporated the following activities and outputs:

- Managing DHIS software at advanced user level, data validation, analysis and feedback to managers (national and provincial sectors);
- Managing and maintaining the national DHIS and its database to ensure there is a constant data flow of reliable and complete data available to users;
- Monitoring the countrywide implementation of DHIS, etc.

To further improve the level of health awareness by making use of technology, the Department of Health decided to develop a South African National Telemedicine System so that it would be able to offer healthcare services to the most distant South African rural areas (“The South African”, n.d.). Patients who usually visit clinics would be able to learn from the content provided by the Telemedicine System. The objective of developing this system was to narrow the gap between the poorly resourced rural areas and the urban areas (National Department of Health, 2004). This technology promised to provide a way of sharing skills

and cutting through problems caused by geographic isolation, poor transport and infrastructure, as well as the scarcity of skilled healthcare professionals ("Ehealth", 2006). This led to a Memorandum of Understanding being signed between Sentech (national signal carrier for both radio and television in South Africa) and the Department of Health in 1999 for the establishment of a Health Channel using satellite technology (National Department of Health, 2004).

The Telemedicine System initiative has helped to improve the level of health awareness in South Africa amongst patients and healthcare workers ("The South African", n.d.). It is probable that health information systems and other technology advancements are viewed as mainly technology acquisition processes aimed at purchasing a turn-key universal solution (Hedberg, 2003). This can cost billions of rands in the end; they should rather be viewed as long-term, socio-cultural, political, and technical development processes with short-term, practical and functional applications that work (Hedberg, 2003). People are the ones that really make technology work. As people form part of the organisational culture, it should not be forgotten how they are to be catered for, or how they should be addressed whenever there is a new technology being introduced within the organisation.

It is essential for the healthcare institutions to ensure that healthcare professionals are able to utilise all the new technologies that the institution initiates. A major determinant of the rate of adoption of information technology in the healthcare sector is the personal computing skills of healthcare professionals; furthermore, if doctors, nurses and other healthcare professionals are comfortable with personal computing, the rate of information technology adoption in healthcare institutions is likely to be faster (Institute of Health Systems, n.d.).

2.5 Conclusion

To reform the South African healthcare sector, the National Department of Health has to evaluate the progress it has made by reflecting on the strategic priorities that it has set and achievements it has brought about over a certain period of time. The National Policy on Quality Assurance should ensure that healthcare received by the citizens of South Africa is of acceptable quality. The South African Government has long realised the need to adjust spending in the healthcare sector so that it can favour the public sector more, as this sector is the one that is utilised by many more people requiring healthcare services.

Investigations into the public and private sectors in South African healthcare showed that the most significant challenge facing the South African healthcare system is to address the inefficient and inequitable distribution of resources between the public and private healthcare sectors relative to the population served by each (McIntyre and Thiede, 2007). Harrison (2007) believes that: a) the private healthcare sector cannot be left to its own devices to exercise the constitutional requirement to achieve the progressive realisation of the right to healthcare, and b) all stakeholders need to recognise the Ministry of Health's responsibility to exercise stewardship over the entire healthcare system, both public and private.

In terms of technology adoption, it is clear that throughout the world, ICT is changing the nature of information dissemination, communication patterns, business practices and economic development (Mechael, 2002). In South Africa and the African context, ICT infrastructures and services should be considered as an integral part of the provision of basic services and a vital catalyst for economic development, competitiveness and growth (National Department of Health, 2004). Much works remains to be done in improving health information systems in South Africa.

As the healthcare sector moves rapidly towards the electronic environment, the issue of rights plays a major role in this regard (e.g. the right to privacy which is a constitutional right). Peoples' confidential medical records can be tampered with by unauthorised and authorised parties; therefore, it becomes increasingly important to secure healthcare information. The next chapter will discuss privacy and security issues that affect the healthcare sector.

Chapter 3

Privacy and Security Issues in the Healthcare Sector

The issues that pertain to the security and privacy of patient information in the healthcare sector will be discussed. First of all, this chapter describes the broader meaning of healthcare information and asks why there is a need for security and privacy in that sector. This is answered by providing a few examples of interesting, past cases showing why security and privacy are important. The terminology used will be explained and the methods of protecting the security and privacy of healthcare information and the legal liabilities involved will be discussed.

"In the long run, preservation of confidentiality is the only way of securing public health." **– Judge Harms (1993) –**

"The choice of speaking is available to me for very particular reasons: because I have a job position that is secure; because I am surrounded by loved ones, friends and colleagues who support me; and because I have access to medical care and treatment that ensures I remain strong, healthy and productive.

For millions of South Africans living with HIV or AIDS, these conditions do not exist. They have no jobs, or their jobs would be at risk if they spoke about their HIV. They not only lack community support, but face grave personal danger if they do so. And, most importantly, they do not have access to proper medical care and treatment. For them, in a still hostile climate, the choices are strictly limited. Their right to invoke confidentiality remains of critical importance to them. It is only by creating conditions in which people can speak out without fear that we can begin to end the silence surrounding South Africans living with AIDS and HIV". **– Judge Edwin Cameron (1999) -**

3.1 Introduction

Providing easier access to and dissemination of healthcare information is necessary as healthcare is moving from the paper-based to the electronic form of data collection (Buckovich et al, 1999). The use of and reliance on electronic information for aiding in all kinds of decision-making processes have reached critical levels in all walks of life ("Media Statement", 2005).

The electronic form of a medical record offers the promise of improved care and increased efficiency (Connecting for Health, 2003). However, the development of guiding privacy, confidentiality, and security principles is necessary in helping to balance the protection of patients' privacy interests against appropriate information access (Buckovich et al, 1999).

Privacy is a valuable aspect of personality ("Media Statement", 2005). New risks to privacy, as well as new means to protect privacy, have been

created by the introduction of information technology into healthcare (Connecting for Health, 2003).

As inevitably technology became accessible to anyone, people are becoming increasingly aware of the privacy issues that involve healthcare information. Many organisations are struggling to develop principles addressing the privacy, confidentiality, and security of healthcare information (Buckovich et al, 1999). Nightly news and spectacular cover stories are made up by the violations of data security and an individual's right to privacy (Wilson, 2002).

There are many issues that emerge when dealing with healthcare information. Issues like the protection of privacy, laws and the sense of security of an individual come into play. The obstacles encountered by healthcare organisations need to be addressed in detail. The next sections of this chapter will initially discuss healthcare information and the various factors that affect this and end off by looking at the legal liabilities thereof.

3.2 Healthcare Information

Such is the nature of the healthcare industry that it administers around the clock, responding to the needs of millions of people – from newborns to the critically ill by combining medical technology and the human touch (U.S. Department of Labor, 2005). Establishments that make up the healthcare industry vary in terms of size, staffing patterns and organizational structures (U.S. Department of Labor, 2005). These establishments have one feature in common: utilising healthcare information.

Healthcare information is any data relating to a person's past, present or future health, or the payment for healthcare ("HIPAA FAQs", n.d.). The information contained in patient records is the core of what is often

understood to be **healthcare information.** Whether on paper or in electronic form, this is the information about patients generated and maintained throughout the healthcare industry in providing health services (NTIS, 1993). Extensive medical records are now kept on computers by both hospital authorities and private insurers, alike ("Media Statement", 2005). This leads to a need for suitable measures to protect these records.

The essence of information protection is to provide a person with (a degree of) control over his or her personal information in instances where his or her personal information is being collected, stored, used or communicated by another person or institution ("Media Statement", 2005). The next section will discuss why there is a need for security and privacy in the healthcare environment.

3.3 The Need for Security and Privacy in Healthcare

The growth of managed care and integrated delivery systems, the rise in the number of entities and people accessing healthcare information for various reasons, and legislative developments such as the Health Insurance Privacy and Accountability Act of 1996 (HIPAA) are some of the many factors contributing to awareness of the need for privacy and security of healthcare information (Buckovich et al, 1999). Data or information protection forms an element of safeguarding a person's right to privacy ("Media Statement", 2005).

There have been many incidents that have caused a lot of havoc in terms of security and privacy of healthcare information and have made the public more aware about their healthcare privacy rights. Here are some every-day examples (Wilson, 2002):

- A celebrity is admitted into a New York City hospital. A data security check identifies over 1,000 hits on her medical record by hospital employees in the first four hours.
- An 80-year-old volunteer in a mid-western community hospital sends a birthday card to every hospital employee on his/her birthday. She obtained this information by accessing the payroll system.
- A concerned mother, working in the business office of an academic medical centre, accesses the medical information of her daughter. Her daughter is 35-years-old and is under psychiatric treatment for drug abuse.

Below are two South African examples.

Dr. Manto Tshabalala-Msimang has served as the South African Health Minister from 1999 and is expected to serve until 2009. In August 2007, a big South African newspaper (*Sunday Times*) ran an article, entitled "Manto's Hospital Booze Binge", about her previous hospital stay at the Cape Town Medi-Clinic in 2005 for a shoulder operation. It was alleged that she had abused her power as a minister by consuming excessive amounts of alcohol and that she had mistreated hospital staff members by ordering them to do things that were not part of their duties (i.e., sending them to buy alcohol for her at night). Tshabalala-Msimang then threatened to take legal action against the newspaper on the grounds that it was in possession of her confidential medical records. She had come to this conclusion as the paper published news about her health status. The *Sunday Times* affirmed that it was really in possession of her confidential medical records. Tshabalala-Msimang was correct to exercise her right as such possession is an offence under the South African National Health Act (SANHA). Tshabalala-Msimang called upon the paper to hand over to her, within 24 hours, all records concerning her hospitalisation, medical treatment, condition and the comments by various doctors.

Tshabalala-Msimang stated in her affidavit to the court that various terms of the SANHA had been violated. These included ("Paper Returns Records", 2007):

- The obligation of a clinic to keep records of all patients;
- The right of a patient to have medical information kept confidential; and
- The obligation of healthcare workers not to disclose medical information unless for legitimate purposes.

Manto Tshabala-Msimang further stated "I have a clear right to my privacy and dignity and to protect those rights. Unless the records are returned, I will suffer irreparable harm to my dignity and reputation." ("Paper Returns Records", 2007).

The worst possible aspect of this event from privacy's perspective is the fact that the hospital only discovered that all Tshabala-Msimang's confidential medical records were missing from its archives after the controversial article was published by the *Sunday Times*. The full judgement of the case was not published as it was only made available to interested parties afterwards. Only the *Sunday Times* was punished by the Johannesburg High Court as it had to: a) return all medical records of Tshabala-Msimang to the Cape Town Medi-Clinic, b) delete all medical records on journalists' laptops and computers, and c) pay the costs in the court case ("Delete Manto Records", 2007). The only action Medi-Clinic took after discovering about the missing records was to lay a complaint of theft with the police ("Top Cop Probing Manto's Records", 2007). Based on this, it is conceivable that the Cape Town Medi-Clinic has not been punished, which is bad, considering the fact that this would have been a good example for other healthcare organisations which might commit the same misdemeanour in the future.

Table 3-1 supplies a short summary of another case dealing with privacy that occurred in 1993.

Table 3-1: The "McGeary Case". Source University of the Witwatersrand (2004)

Case: Jansen van Vuuren and Another NNO v Kruger 1993 (4) SA 82 (A)
Mr. McGeary went to his doctor for an HIV test. The test showed Mr. McGeary had HIV. The next day, his doctor was playing golf with another doctor and a dentist and told them that Mr. McGeary had HIV. **The court found that this was a violation of Mr. McGeary's rights because:** ▪ Doctors must keep this information private or else people will not go to them for tests and treatment. Telling other doctors about a patient's HIV status will not stop the transmission of HIV; ▪ Doctors must follow the South African Medical & Dental Council (SAMDC) Guidelines, which say that they should not tell anyone your HIV status unless you consent to this; and ▪ It is important to keep this information private because people with HIV are often discriminated against.

From the above examples, it is clear there is a need to ensure that healthcare information is protected by every healthcare organisation. They need to do this in order to ensure that the public retains faith in the healthcare sector.

It must be noted that each and every patient that enters a healthcare institution has privacy rights.

Rights are valued, and principles such as freedom, equality, respect and dignity guide communities and societies as to how people should behave and treat each other. Slack et al (2000) state that the philosophies of inalienable birth or human rights have been translated into international documents such as the 1948 Universal Declaration of Human Rights and, in many cases, into law. Since each person has the **right to privacy**, they can decide to whom they want to tell what (University of the Witwatersrand, 2004). In the South African context, this right is embodied in the **Constitution**, which is the highest law in the country. There is no

law or policy that is allowed to go against this right and everyone in the country has to follow it (University of the Witwatersrand, 2004).

Other countries do have structures in place to address the privacy of personal information. For instance in Australia, there are ten National Privacy Principles (NPPs) as extracted from the Privacy Amendment (Private Sector) Act 2000. Below is a table with a brief overview of these principles.

Table 3-2: National Privacy Principles in Australia. Source The Office of the Privacy Commissioner (n.d.)

Principle	Definition
1: Collection	An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.
2: Use and Disclosure	An organisation must not use or disclose personal information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose of collection unless: …
3: Data Quality	An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.
4: Data Security	An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.
5: Openness	An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.
6: Access and Correction	If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that: …
7: Identifiers	An organisation must not adopt as its own identifier

	of an individual, an identifier of the individual that has been assigned by: …
8: Anonymity	Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.
9: Transborder Data Flows	An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if: …
10: Sensitive Information	An organisation must not collect sensitive information about an individual unless: …

The issue of patient rights with regards to healthcare information in South Africa is discussed further in Section 3.5.4 of this study, which deals with the Draft Privacy Bill.

Notwithstanding the privacy rights that patients have, the law nevertheless allows for the use and disclosure of the patient's protected health information for purposes of treatment, payment and healthcare operations (Samaritan Health Services, n.d.), as illustrated in Table 3.3.

Table 3-3: Examples of Use and Disclosure of Protected Health Information for Treatment, Payment and Health Operations. Source Samaritan Health Services (n.d.).

Operation	Example
For Treatment	▪ Information obtained by a nurse, physician, or other member of a healthcare team can be recorded in a patient's medical record and used to help decide what care may be right for the patient. ▪ Information may be provided to others providing care for the patient. This will help them stay informed about the patient's care.
For Payment	▪ Payment is requested from the health insurance

	plan. Health plans need information from the health service provider about the patient's medical care. Information provided to health plans may include diagnoses; procedures performed, or recommended care.
For Healthcare Operations	▪ The patient's medical records are used to assess quality and to improve services. ▪ The medical records may be used and disclosed to review the qualifications and performance of the health service provider's healthcare providers and to train the healthcare provider's staff. ▪ The patient may be contacted to be reminded about appointments and given information about treatment alternatives or other health-related benefits and services. ▪ The patient may be contacted by the healthcare service provider to raise funds. ▪ The patient's information may be used and disclosed to conduct or arrange for services, including: o medical quality review by the patient's health plan; o accounting, legal, risk management, and insurance services; o audit functions, including fraud and abuse detection and compliance programs

However, while laws will allow the use and disclosure of information as detailed in Table 3.3, it also details the requirements for ensuring the security and confidentiality of **protected health information** (PHI) (Wellsource, 2005).

From this section it is evident that privacy rights and legal obligations are important drivers in the protection of healthcare information. This protection of healthcare information is of paramount importance because (Medical College of Georgia, n.d.):

- Healthcare providers rely on healthcare information to process claims, coordinate care (portability) and for other administrative functions;
- Individuals are concerned how their information is used;
- Patients want to know that their sensitive information will be protected;
- In order to receive accurate and reliable diagnosis and treatment, patients must provide accurate, detailed information about their personal health, behaviour and other aspects of their lives (which they may not do if they are indecisive about protection of their privacy).

Bearing the afore-mentioned factors in mind, healthcare organisations need to know more about the protection of security and privacy of healthcare information. The next section will discuss this protection of security and privacy.

3.4 Protecting the Security and Privacy of Healthcare Information

Clarke (1993) states that information security has always been an important concern for government agencies. Furthermore, patients are well aware of the potential risks associated with the automation and sharing of their medical information (Connecting for Health, 2003). If there is no sound information security in place, these concerns can lead patients to withhold from their clinicians healthcare information that could be crucial for their care (Connecting for Health, 2003).

Out of the 344 physicians in a survey that was conducted by the Association of American Physicians Surgeons (AAPS) in 2003, 96 percent of them thought that implementing privacy rules would further compromise patient privacy (AAPS, 2001). If physicians themselves are hesitant of the privacy rules that must be implemented, how much more are the patients? Doctors do lie to protect patient privacy. Below is a summary of the findings from the survey (AAPS, 2001):

- Nearly 87% of physicians reported that a patient had asked that information be kept out of the record;
- Nearly 78% said that they had indeed withheld information from a patient's record due to privacy concerns;
- Only 19% admitted to lying to protect a patient's privacy; and
- 74% stated that they had withheld information to protect a patient's privacy.

It is clear that principles about security and privacy still have to be instilled in the individuals that deal with healthcare information and the individuals whose information is dealt with. This will be beneficial to all concerned stakeholders in the long run.

As a precursor to examining the legal liability with regard to security and privacy in healthcare, it is considered appropriate to provide some discussion on the distinction between the concepts of **security**, and **privacy**.

3.4.1 Security

Wilson (2002) describes **security** as the protection of data resident on provider computers or networks, as well as the protection of data while it is being transmitted to third parties; primarily the technical components that address the collection, protection, and dissemination of data.

Clarke (1993) describes **security** as:

- Protection against unauthorised use of, access to or disclosure of personal information, including measures designed to prevent, to detect and to enable investigation of unauthorised use, access and disclosure; and
- Assurance of the appropriateness of information-handling procedures in achieving those aims.

In the area of information security, the term is often divided into three components: confidentiality, integrity and availability. A brief discussion of these components follows.

3.4.1.1 Confidentiality

Confidentiality is the property that data or information is not made available or disclosed to unauthorized persons or processes (University of California San Francisco, 2005). According to Buckovich et al (1999), confidentiality is the status afforded to data or information indicating that it is sensitive for some reason, and therefore it needs to be protected against theft, disclosure, or improper use, or both, and must be disseminated only to authorized individuals or organizations with a need to know.

In the healthcare context information must be available strictly on a 'need-to-know' basis and therefore the confidentiality of this information must be protected as a fundamental requirement.

3.4.1.2 Integrity

Integrity is the property that data or information has not been altered or destroyed in an unauthorized manner (University of California San Francisco, 2005). Integrity of information is imperative in healthcare as it is used to guide healthcare staff members with decision-making. If

healthcare information that healthcare staff members base their decisions on is incorrect, it can result in hazardous events like the death of patients, or patients being given wrong medication.

3.4.1.3 Availability

Availability is the property that data or information is accessible and usable upon demand by an authorised person/entity (University of California San Francisco, 2005). For healthcare organisations to function properly, healthcare information needs to be accessed by authorised stakeholders whenever the need arises. Healthcare organisations, therefore, must ensure that the availability of this information is not compromised.

The three elements of security (confidentiality, integrity and availability) play a very important role in healthcare. However, healthcare organisations need to comprehend that ensuring the security of healthcare information does not necessarily guarantee its privacy. Privacy of healthcare information must be ensured as this involves various authorised stakeholders, i.e., healthcare staff members that are able to access such information.

3.4.2 Privacy

Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define (South African Law Reform Commission, 2005). **Privacy** is the right of individuals to be left alone and to be protected against physical or psychological invasion or the misuse of their property (Buckovich et al, 1999). It includes freedom from intrusion or observation into one's private affairs, the right to maintain control over certain personal information, and the freedom to act without outside interference (Buckovich et al, 1999). It also provides information to patients on their own information and where that is being used. Then there is also **information privacy,** which Clarke (1993) defines as the interest that

individuals have in knowing about, and controlling, or at least constraining, the handling of personal information about themselves, including its collection, storage, dissemination and use.

Personal information about a patient, learnt both inside and outside of the healthcare establishment, shall be kept confidential at all times unless the patient gives consent, there is legal justification for disclosure or where a real risk of serious harm, injury or damage to third party/public exists (Occupational Therapy Association of South Africa, 2005). If this consent is not given, it will be considered as an invasion of the patient's privacy. A case in point is the example of the Manto Tshabalala-Msimang incident discussed in Section 3.3. The following section will discuss the legal liabilities that come with the handling of information of such a nature.

3.5 The Legal Liability

Concern about information protection has increased worldwide since the 1960s as a result of the expansion in the use of computer and telecommunications' technologies ("Media Statement", 2005). The author continues by stating that worldwide, the surveillance potential of powerful computer systems has prompted demands for specific rules governing the collection and handling of personal information.

The healthcare sector is very complex as it deals with various factors, like peoples' sensitive information and other information of a similar nature. With these come different challenges, one of which is to comply with the legal acts that may be in place in a particular country.

There are now well over 30 countries that have enacted information-protection statutes at national or federal level and the number of such countries is steadily growing ("Media Statement", 2005). Harvey (2007) quotes the World Health Organization as stating that Australia, New Zealand, Canada and the United States of America have some of the

world's best-run and best-funded healthcare sectors (World Health Organization Statistical Information System, 2007). This study will take a look at some of the legislation that was set up to address privacy issues in these countries. Examples are **Canada** (**Privacy Act 1983** and **Personal Information Protection and Electronic Documents Act**, **2000**), **Australia** (**Privacy Act**, **1988** and **The Privacy Amendment** (**Private Sector**) **Act 2000**), **New Zealand** (**Privacy Act 1993**) and **United States of America (Health Insurance Portability and Accountability Act 1996)**. Below is a brief summary of these acts.

Canada

The Privacy Act 1983: the purpose of this act is to extend the present Canadian laws that protect the privacy of individuals with respect to personal information about themselves held by a government institution and provide individuals with a right of access to that information (Office of the Privacy Commissioner of Canada, 2003).

The Personal Information Protection and Electronic Documents Act 2000 (PIPEDA): addresses the collection, storage and use of personal information by organizations in the private sector (Privacy Commissioner of Canada, 2007). Its provisions apply to information collected, used or disclosed by federally regulated agencies such as telecommunications companies, ISPs, broadcasters, airlines and banks (Privacy Commissioner of Canada, 2007).

Australia

The Privacy Act 1988: makes provision to protect personal information in the hands of federal government agencies ("Privacy Act 1988", 2006).

The Privacy Amendment (Private Sector) Act 2000 amended the Privacy Act 1988 to regulate some private-sector organisations/businesses ("Privacy Amendment Act", 2000), but not all of them. It was passed by Parliament in December 2000 and became operative on 21 December 2001; some provisions did not commence until 21 December 2002

(Electronic Frontiers Australia, 2006). The ten National Privacy Principles (NPPs) contained in the Australian Privacy Amendment (Private Sector) Act 2000, were provided in Table 3.2 (Section 3.3) earlier in this Chapter.

New Zealand

The Privacy Act 1993: applies across the public and private sectors in New Zealand. It has as one of its main purposes the promotion and protection of individual privacy in general accordance with the 1980 Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (The Office of the Privacy Commissioner in New Zealand, n.d.).

United States of America

HIPAA (Health Insurance Portability and Accountability Act of 1996): is a set of federal rules designed in part to protect the privacy of a person's healthcare information ("HIPAA FAQs", n.d.). The objectives of the act are to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and healthcare delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes ("Health Insurance Portability and Accountability Act of 1996", 1996).

South Africa

The investigation into the development of information privacy legislation for South Africa is, therefore, in line with international trends ("Media Statement", 2005). South Africa has no general data protection law in place that deals with privacy (Michalson & Hughes, 2005); however, there are certain stipulations in some legal documents that deal with privacy. At the moment, there is only a Draft Privacy Bill which is not law yet. South African healthcare organizations must ensure that they comply with the South African National Health Act (SANHA), the Electronic Communication Transaction Act (ECTA) requirements, and Promotion of Access to

Information Act (PAIA) to ensure due care and due diligence practices (Tuyikeze, 2006).

South Africa cannot afford to be denied general access to personal information from its major trading partner countries, most of which have already implemented proper information protection legislation ("Media Statement", 2005). In the next sections, acts that deal with privacy in South Africa will be briefly discussed as well as the Draft Privacy Bill of South Africa.

3.5.1 The Promotion of Access to Information Act

The Promotion of Access to Information Act 2 of 2000 (PAIA) was assented to by the President of South Africa on 2 February 2000. The PAIA was enacted in accordance with section 32 (2) of the South African Constitution. This act represented a landmark in South African history, addressing, for the first time, the pre-1994 culture of secrecy in state and private institutions, seeking to foster a culture of transparency and accountability in South Africa ("Access to Information Guide", 2005). The act also acknowledged the need to educate South Africans on their rights, to enable them to participate in decision-making that affects their lives ("Access to Information Guide", 2005). The act affects both private and public bodies. The South African Human Rights Commission is playing a key role in the implementation of the PAIA.

The PAIA gives any person the right of access to (South African Human Rights Commission, n.d.):

- Any information held by the State; and
- Any information that is held by another person and that is required for the exercise or protection of any rights.

This means that a person can request access to information held by public bodies, as well as from a natural or juristic person (private body) (South

African Human Rights Commission, n.d.). The South African Human Rights Commission (n.d.) further states that in the case of a request for access to information held by a natural or juristic person, it has to be indicated that the information requested is required for the exercise or protection of any rights.

The right of access to information is a person's right in terms of section 32 of the Constitution, and the PAIA gives effect to section 32, by amongst others (South African Human Rights Commission, n.d.):

- Providing and detailing the procedures that must be followed in order to make a request for information;
- Stating from whom you can make a request;
- Detailing the duties of the bodies, from whom you have made a request;
- Describing what information can be requested;
- Describing when the requested information must / may be refused;
- Describing what mechanisms and procedures are available to a person if their request for access to information is refused.

The PAIA is usually effective when it comes to court cases. Section 50 of the act provides that a person must be given access to any record of a private body if that record is required for the exercise or protection of any rights (Price, n.d.). In the recent decision of *Unitas Hospital v Van Wyk [2006] SCA 32 (RSA),* the Supreme Court of Appeal considered a request for access to a record under the provisions of the PAIA and commented on the interpretation of "required" in section 50 (Price, n.d.).

3.5.2 The Electronic Communications and Transaction Act (No. 25 of 2002)

The Electronic Communications and Transaction Act 25 of 2002 (ECT Act) was assented to by the President of South Africa on the 31 July 2002. The act came into effect on 30 August 2002. This marked the end of a process

initiated by the South African Government in 1999 to establish a formal structure to define, develop, regulate and govern e-commerce in South Africa (Tuyikeze, 2006).

The objectives of the ECT Act (ECT Act, 2002) are:

- To provide for the facilitation and regulation of electronic communications and transactions;
- To provide for the development of a national e-strategy for the Republic;
- To promote universal access to electronic communications and transactions and the use of electronic transactions by SMMEs;
- To provide for human resource development in electronic transactions;
- To prevent abuse of information systems;
- To encourage the use of e-government services;
- And to provide for matters connected therewith.

The ECTA consists of 14 chapters with 95 sections. Here is a brief of some content within the chapters (ECT Act, 2002):

I. **Chapter 1.** "Interpretation, Objects and Application" explains definitions used in the act, and the objectives of the act;
II. **Chapter 2.** "Maximising Benefits and Policy Frameworks" requires the Minister to set up a national e-strategy, promotion of universal access and assistance of SMMEs to utilise electronic transactions;
III. **Chapter 3.** "Facilitating Electronic Transactions" deals with the legal requirements and communication of data messages;
IV. **Chapter 4.** "E-Government Services" describes the acceptance of electronic filing and issuing of documents as well as the requirements that may be specified by notice;
V. **Chapter 5.** "Cryptography Providers" requires that the Director-General maintain a list of cryptography providers and that these providers register with the Department of Communications;

VI. **Chapter 6.** "Authentication Service Providers" states that there must be an Accreditation Authority which will deal with all issues that come up in the accreditation cycle;

VII. **Chapter 7.** "Consumer Protection" requires vendors to provide consumers with a minimum set of information and the right to withdraw an electronic transaction before it is completed;

VIII. **Chapter 8.** "Protection of Personal Information" deals with the scope of protecting personal information and principles for electronically collecting personal information;

IX. **Chapter 9.** "Protection of Critical Databases" compels the Minister to determine requirements and procedures to follow for the registration and management of critical databases;

X. **Chapter 10.** "Domain Name Authority and Administration" has the following parts dealing with: 1) the establishment and incorporation of the .za domain name authority, 2) the governance and staffing of this authority, 3) the functions of this authority, 4) the financial issues of the authority, 5) regulations regarding the authority and 6) alternate dispute resolution ;

XI. **Chapter 11.** "Limitation of Liability of Service Providers" mentions how the Minister may recognise a representative body for service providers based on some criteria. Service providers are also protected based on conditions, if some unlawful events that might occur;

XII. **Chapter 12.** "Cyber Inspectors" allows the Director-General to appoint cyber inspectors that will monitor Internet websites in the public domain and see to it that cryptography and authentication service providers comply with the relevant provisions of this act;

XIII. **Chapter 13.** "Cyber Crime" defines the context of access and then mentions unauthorised access and interference with data can result in a crime and the penalties thereof;

XIV. **Chapter 14.** "General Provisions" has provisions which give jurisdiction to courts trying an offence in terms of this act.

The ECT Act places a heavy burden on medical providers, insurers and claims clearinghouses, as well as other healthcare services partners who

need to communicate electronically on a day-to-day basis to accomplish their tasks with the increased use of electronic communication transactions in healthcare business transactions (Tuyikeze, 2006). In the context of security and privacy in the health sector, Chapter 8 of the ECT Act which deals with the protection of personal information, is directly relevant. Personal information elicited through electronic transactions is given special protection in terms of this chapter which requires, inter alia, the written permission of the owner of that information to the collection and use thereof by the website owner, and prohibits the collection and retention of information which is irrelevant or obsolete (and by implication, any "trafficking" in such information (“The Electronic Communications and Transactions Act”, 2003).

3.5.3 The South African National Health Act (No. 61 of 2003)

The South African National Health Act 61 of 2003 (SANHA) was acquiesced to by the President on 18 July 2004. The objective of the act is to provide a framework for a structured uniform health system within the Republic, taking into account the obligations imposed by the Constitution and other laws of the national, provincial and local governments with regard to health services; and to provide for matters connected therewith (SANHA, 2004).

The SANHA comprises of 12 chapters with 90 sections. A brief summary of the chapters is provided below (SANHA, 2004):

I. **Chapter 1.** “Objects of Act, Responsibility for Health and Eligibility for Free Health Services in Public Health Establishments” allows the Minister of Health to: orchestrate the National Health System, be responsible for health within the limits of available resources and, upon consultation with the Minister of Finance, might be eligible to provide free health services for the public in public-health establishments;

II. **Chapter 2.** “Rights and Duties of Users and Healthcare Personnel” defines rights of the general public as well as those of the healthcare personnel;

III. **Chapter 3.** “National Health” portrays the general functions of the National Department of Health and the establishment of the National Health Council;

IV. **Chapter 4.** “Provincial Health” determines provincial health services and summarises the establishment, composition and the functions of the Provincial Health Council;

V. **Chapter 5.** “District Health System” deals with the establishment of district health systems, division of health districts into sub-districts and the establishment of district health councils amongst others;

VI. **Chapter 6.** “Health Establishment” deals with the classification of health establishments and the issues that pertain to the certificate of need, the evaluation and the relationship between the public and private heath establishments is also dealt with;

VII. **Chapter 7.** “Human Resources Planning and Academic Health Complexes” touches on the development and provision of human resources in the national health system and the regulations relating to human resources;

VIII. **Chapter 8.** “Control of Use of Blood, Blood Products, Tissue and Gametes in Humans” takes a look at issues that concern the removal and use of tissue, blood, blood products or gametes withdrawn from living persons;

IX. **Chapter 9.** “National Health Research and Information” states that there must be a National Health Research Ethics Committee and National Health Research Ethics Council established at every institution, health agency and health establishment where health research is carried out;

X. **Chapter 10.** “Health Officers and Compliance Procedures” deals with the appointment of health officers responsible for inspecting health establishments for compliance to this act as recommended by the office of standards compliance;

XI. **Chapter 11.** "Regulations" gives the Minister the power to regulate on various issues covered in this act;

XII. **Chapter 12.** "General Provisions" allows the Minister to establish advisory and technical committees after consultation with the National Health Council, should the Minister feel it is necessary to do so in order to achieve the object of this act.

Chapter 2 of the SANHA ("Rights and Duties of Users and Healthcare Personnel") contains a number of provisions addressing the protection of the security and privacy of health information. In this chapter, it is stated that a person may not be refused emergency treatment, must be informed of their health status, diagnostic procedures, risks, and their right to refuse health services, and be informed in a language that they understand and their level of literacy must be considered (SANHA, 2004). It is further stated that a person must give consent before being provided a health service and they must participate in any decisions that are taken with regards to their health. Some of the aspects that are included in this chapter are: the duty to disseminate information, the obligation to keep records, the confidentiality of health information, the access and protection of health records, the laying of complaints and the duties of a person when they are utilising the health services of an establishment.

3.5.4 Draft Privacy Bill

The South African Law Reform Commission released a Discussion Paper entitled "Privacy and Data Protection" in October 2005. This paper was accompanied by a Draft Privacy Bill for South Africa. This Draft Privacy Bill has not been made law yet. The Draft Privacy Bill has two objectives: a) to promote the protection of personal information processed by public and private bodies; b) to provide for the establishment of an Information Protection Commission; and to provide for matters incidental thereto (South African Law Reform Commission, 2005).

Under the general provisions of the Draft Privacy Bill, the objectives are very clear when it comes to privacy. Table 3-4 sheds more light on Section 1 of this Draft Privacy Bill which deals with the objectives.

Table 3-4: Objects of the Act, Section 1. Source South African Law Reform Commission (2005)

Subsection	Definition
(1)	The objectives of this act are: a)) to give effect to the constitutional right to privacy i. by safeguarding a person's personal information when processed by public and private bodies; ii. in a manner which balances that right with any other rights, including the rights in the Bill of Rights in Chapter 2 of the Constitution, particularly the right to access to information; iii. subject to justifiable limitations, including, but not limited to effective, efficient and good governance and the free flow of personal information, particularly trans-border transfers. b) to establish voluntary and mandatory mechanisms or procedures which will be in harmony with international prescripts and which will, while upholding the right to privacy, at the same time contribute to economic and social development in an era in which technology increasingly facilitates the circulation and exchange of information; and c) generally, to promote transparency, accountability and effective governance of all public and private bodies by, including, but not limited to, empowering and educating everyone to understand their rights in terms of this act in order to exercise their rights in relation to public and private bodies.

South Africa has limited legislation to help enforce privacy in the health sector as compared to developed nations such as Australia, New Zealand and Canada who have some of the most advanced legislative frameworks when it comes to the privacy of patient information (Harvey, 2007). Therefore the development of the Draft Privacy Bill can be seen as a step in the right direction.

3.6 Conclusion

In this chapter, the nature of healthcare information and the importance of protecting its security and privacy, were established. Some incidents illustrating the violation of the security and privacy of healthcare information, were discussed. It was further asserted that the protection of health information is not only required as a best practice, but due to the legal framework that a country establishes for the protection of such information.

With consideration for the fact that the success of initiatives to secure and protect the privacy of information, depends to a great extent on the people that are involved, this brings the discussion now to the crux of this research, namely information security education, training and awareness. The human factor is a sizeable factor which if ignored, can render any information security programme useless; hence, the next chapter will investigate security education, training and awareness for employees in the healthcare environment.

Chapter 4

General Security Education Training and Awareness Principles

This chapter discusses the general principles of Information Security Education, Training and Awareness (SETA). It defines SETA and the different elements that are included in it. It then provides a brief overview of the process of designing, developing and implementing a SETA programme.

"The big lie of computer security is that security improves by imposing complex passwords on users. In real life, people write down anything they can't remember. Security is increased by designing for the way humans actually behave." **- Jakob Nielsen -**

"If I were a terrorist or criminal who wanted to disrupt and steal from your company, I would look at your vulnerability through your staff." **– Alastair Morrison –**

"The biggest challenge in maintaining IT security is overcoming staff complacency" **– Peter Pederson -**

"*Just as steps have been to taken to ensure the safety of the employees in the workplace, the organization is now asking that the employees work to protect the second most important enterprise asset - information. If the organization fails to protect its information from unauthorized access, modification, disclosure and/or destruction, then the organization faces the prospect of loss of customer confidence, competitive advantage and possibly jobs. All employees must accept the need and responsibility to protect our property and assets."* **– Melissa Guenther (2001) -**

4.1 Introduction

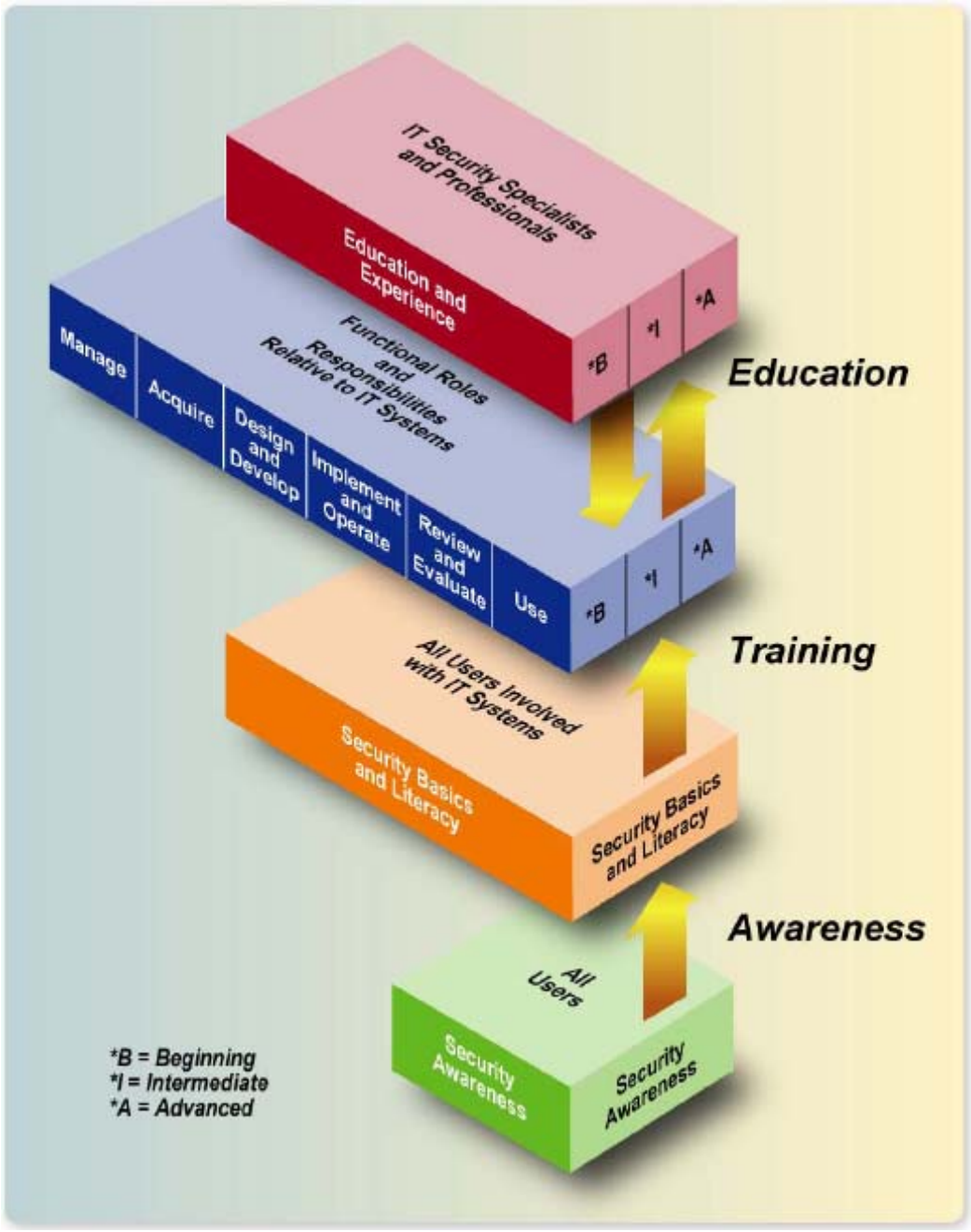
CIOs, managers and staff are faced with ever increasing levels of complexity in managing the security of their organisations and in preventing attacks that are increasingly sophisticated (Garrett, 2004). Information is the lifeblood of organisations, a vital business asset in today's IT-enabled world (Hinson, 2005). More often than not, it has been proven beyond doubt that in the modern society, ignorance can be hazardous. Protecting and enhancing the value of information and IT systems have become central objectives in most businesses, second only to making profits (Hinson, 2005). Programs and systems are habitually being utilised by the computer users that are not aware of the peril that their possible ignorance might cause. However, as stated by Gary Hinson,

“Ignorance and apathy are not incurable conditions”. Ignorance is one of the reasons why organisations have realised that it is imperative for them to teach their employees about information security. This is normally addressed by a SETA programme.

A SETA programme consists of three elements: awareness, training and education. The purpose of computer-security awareness, training, and education is to enhance security by: improving awareness of the need to protect system resources; developing skills and knowledge so computer users can perform their jobs more securely; and building in-depth knowledge, as needed, to design, implement, or operate security programs for organisations and systems (NIST 800-50, 2003).

As shown in Figure 4.1, below. The learning of a SETA programme is a continuum (NIST 800-16, 1998). The learning continuum has three levels. It starts with awareness, constructs to training and then develops into education.

Figure 4.1: The Learning Continuum. Source NIST 800-50 (2003)



Awareness: As the learner is only the recipient of information and does not actively participate (NIST 800-16, 1998), the purpose of an awareness programme is to stimulate and motivate those being trained to care about security and to remind them of important security practices (NIST 800-50, 2003). Posters and flyers are very helpful in assisting with this level of the learning continuum.

Training: Training focuses on providing the knowledge, skills, and abilities specific to an individual's role and responsibilities relative to IT systems (Federal Agency Security Practices, 2000). There are usually two groups of users that are targeted for training: the general users and the advanced users or users with specialised skills.

Education: This level of the learning continuum integrates all of the security skills and competencies of the various functional specialities into a common body of knowledge (NIST 800-16, 1998). Most organisations opt not to include information security education as part of their SETA programmes as it is part of employee career development.

In the remaining sections of this chapter, the three levels of the learning continuum and the various factors that affect these levels will be investigated.

4.2 Awareness

4.2.1 Background

The term "information security awareness" is used to refer to a state where users in an organisation are aware of – ideally committed to – their security mission (often expressed in end-user security guidelines) (Siponen, 2000). Richard Bland College Information Technology Services (2004) describes information security awareness as understanding the current risks which users may encounter on a day-to-day basis and knowing what to do. Gilbert (2003) defines it as a learning process that changes individual and organisational attitudes and perceptions to realize the importance of security and the adverse consequences of its failure. Each individual who has access to electronic protected health information

must be aware of the appropriate security measures to reduce the risk of improper access, uses, and disclosures (CalOHI Office of HIPAA Implementation, 2005). Security-*awareness* programmes: (1) set the stage for *training* by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure; and (2) remind users of the procedures to be followed (NIST 800-12, 1995).

Raising the awareness of employees' knowledge of security and getting them to understand their own role in security cannot happen with a one-time event, but rather requires the development of a continuous process (Munley, 2004). Awareness goals at the end-user level are to help them: a) understand information security and privacy risks and the actions to reduce them; and b) create a demand for risk reduction (Herold, 2003). Awareness activities should (Herold, 2003):

- Occur on an ongoing basis;
- Use a wide range of delivery methods;
- Catch the attention of the target audience
- Be less formal than training;
- Take less time than training;
- Be creative, memorable and fun;
- Reinforce the lesson learned during formal training.

4.2.2 The Importance of Security Awareness in an Organisation

Nowadays, information and technology have become critical factors to help organisations to succeed with their business functions (Kruger and Kearney, 2006). Safeguarding information and systems, as well as other assets, requires security activity to be organized efficiently across the organisation (Guenther, 2001a). Swanson and Guttmann (1996) argue that in a private-sector business, having good security is usually secondary to the need to make profit. However, security ought to increase

the firm's ability to make a profit. The authors say that in a public-sector agency, security is usually secondary to the agency's providing services to citizens. Similarly, security ought to help improve the service provided to the citizens. So from this, it is clear that an organisation's security budget has to be spent wisely, or security awareness will not be deemed as necessary by many organisations. Raising security awareness in an organisation can spare it from potential humiliation by authorised and unauthorised stakeholders.

Awareness will stimulate and motivate those being trained to care about security and to remind them of important security practices (NIST 800-12, 1995). Information-security awareness activities promote ongoing compliance as they can occur everywhere and on a continuous basis (Herold, 2003). Ongoing compliance helps ongoing awareness as a security programme will be most effective when employees practice security daily (U.S Department of Commerce, 2003). Information security policies are necessary to ensure that important data, business plans and other confidential information are protected from theft or unauthorized disclosure (Kaur, 2001). A SETA programme should communicate the IT security policy to each IT user and assure a complete understanding of the importance of IT security (Arkansas' Enterprise Architecture, n.d.). By being aware of organisational policies, employees will know what is expected of them and how to handle confidential organisational information (Kaur, 2001). If employees are not informed of applicable organisational policies and procedures, they cannot be expected to act effectively to secure computer resources (NIST 800-12, 1995). So it is very important that all employees of an organisation be educated and be trained in organisational policies (Kaur, 2001).

Clearly, many organisations are cognisant of the importance of information and information assurance to the value of their business, and organisations are moving to respond to threats (Garrett, 2004). Many organisations have established information-security awareness

programmes to ensure that their employees are informed and aware of security risks, thereby protecting themselves and their profitability (Kruger and Kearney, 2006). Explaining what happens to an organisation, its mission, customers and employees if security fails motivates people to take security seriously (NIST 800-12, 1995).

Employees must be encouraged to think security into every action they take and every decision that they make (Guenther, 2001b). The SETA programme should convey the message that IT security is to the benefit of the organisation, all its employees, and that everybody is responsible for it (Arkansas' Enterprise Architecture, n.d.). One of the keys to a successful SETA programme is security awareness and training (NIST 800-12, 1995).

Management sets the example for behaviour within an organisation ("Lesson 12", 2006). The IT security-awareness programme should be supported by, and represent the view of management (Arkansas' Enterprise Architecture, n.d.). This is due to the intensified need for improved information security (Kruger and Kearney, 2006). Appropriate awareness for management officials might stress management's pivotal role in establishing organisational attitudes toward security ("Lesson 12", 2006). Management should clearly define roles and responsibilities for personnel, including the requirement to adhere to management policies and procedures, the code of ethics and professional practices (Arkansas' Enterprise Architecture, n.d.). If employees know that management does not care about security, no training class teaching the importance of security and imparting valuable skills can be truly effective ("Lesson 12", 2006).

4.2.3 The Human Factor

The major causes of loss due to an organisation's own employees are: errors and omissions, fraud, and actions by disgruntled employees (NIST 800-12, 1995). People are, indeed, a crucial factor in ensuring the

security of computer systems and valuable information resources ("CSL Bulletin", 1993). Human actions account for a far greater degree of computer-related loss than all the other sources combined ("Lesson 12", 2006). Of such losses, the actions of an organisation's insiders normally cause far more harm than the actions of outsiders (NIST 800-12, 1995). Computer users can naively open email attachments that may be disguised as legitimate correspondence, or they may be convinced to provide their system account information by official looking requests (Munley, 2004). One principal purpose of security awareness, training, and education is to reduce errors and omissions ("Lesson 12", 2006).

Kevin Mitnick, one of the world's most famous hackers and fugitive turned security experts, considers the human factor the weakest link in security (Mitnick and William, 2002). Unfortunately, many organisations are still focusing primarily on technical solutions such as firewalls, anti-virus software, patches, biometric devices and the like to protect themselves against these threats (Munley, 2004). The *people factor* - not technology - is key to providing an adequate and appropriate level of security (NIST 800-50, 2003).

Regardless of the quantity or sophistication of the security technologies that have been put into place in an organisation, the biggest vulnerability still comes from the people within the company who have access or knowledge about the business and its data (Munley, 2004). Security apathy and ignorance are still the biggest threats to computer systems (Guenther, 2001d). Organisations are also perpetually failing to realise a huge impact that the human factor can play. For the sake of the financial impacts of threats and attacks against these organisations, organisations need to take a holistic approach to security by combining technology with awareness (Munley, 2004). And the best way to achieve a significant and lasting improvement in computer security is not by throwing more technical solutions at the problem – it is by raising awareness and training and educating all computer users in the basics of computer security (Guenther, 2001d). A manner of juxtaposing people and technology and

integrating the two to function properly to the benefit of the organisation is truly necessary.

Schultz (2004), who has been heavily involved in the area of information security for almost two decades, believes that training and awareness can do much more for information security as well as for organisations' business interests as a whole, than they have so far. Awareness audiences are very broad; they include everyone within the organisation and all third parties who do work for, or on behalf of, the organisation (Herold, 2003). According to Herold, (2003), awareness audiences have diverse experiences, backgrounds and job responsibilities.

Too many courses (especially courses taught by independent training organisations) do not properly consider entry behaviours - skills and knowledge necessary to understand the course content that is to be taught - resulting in a ''one-size-fits-all'' approach that leaves many attendees puzzled and many others bored, disappointed, and even hostile because they have learned nothing new (Schultz, 2004). As information security and privacy regulations change, and subsequently information security privacy and security policies and procedures, personnel must be notified (Herold, 2003). In today's systems environment, almost everyone in an organisation may have access to system resources and, therefore, may have potential to cause harm ("Lesson 12", 2006). People are usually the weakest link in the information security chain. It is imperative that the shortcomings of people with regards to information security be properly addressed in order to avoid this weakest link crafted by human beings.

Although the security risks caused by people cannot be totally eliminated, increasing awareness of information security will spread knowledge and thus increase understanding of information security concepts and objectives (NIST 800-50, 2003). The awareness goal at the decision-making level is to convince the audience that information security and privacy-risk reduction is achievable (Herold, 2003).

4.2.4 Security Awareness and Organisational Culture

Most companies are still far from creating a culture of security awareness within their organisations even though aftermaths of events like that of September 11th have brought to the forefront the realisation of security threats being real (Siponen, 2000). Organisations need to instil a serious change of information-security awareness amongst its employees. This change cannot occur overnight, there must be enormous effort and commitment the whole year round to achieve this change. There are three main stages that are key to achieving change (Munley, 2004):

- Understand the current culture of your organisation;
- Define the vision;
- Create a roadmap for implementing the change.

True change comes only when the vision is deeply engrained into the psyche and actions of every employee (Munley, 2004). Organisations can achieve this change by purely making use of SETA programmes.

There is a need to give individuals a greater sense of awareness about their own decision-making skills, knowledge that can be applied in their own organisations to improve judgment about security planning and security-related decisions and help develop behaviours that support a security-aware culture (Garrett, 2004). The ultimate goal is to inspire change to create a culture of security awareness (Munley, 2004). Such a culture should promote an awareness of the importance of securing the information assets of an organisation by (Hinson, 2005):

- Informing people about information-security risks and controls in a general sense, and providing more specific information and guidance where necessary;

- Emphasizing management's support for, and commitment to, information security;
- Promulgating the organisation's information-security policies, standards, procedures and guidelines, and externally imposed laws, rules and regulations;
- Motivating people to behave in a more security-conscious manner, for example, taking security risks into account in business decision-making; and
- Speeding up the identification and notification of security breaches within an organisation.

Irvine et al (n.d.) believe that programmes of information security should cover several major areas. For starters, users should appreciate the impact of poor security choices on the health of the organization; secondly, users should be provided with instruction that help them understand the concrete steps they can take to improve information security within their organisation (Irvine et al, n.d.). An example for a typical user may be as simple as understanding notions such as the value of a good password that is changed periodically; for a technologist, the effect of certain network topologies and connections on security might be addressed. All of this contributes to establishing a security-aware culture in organizations. However, awareness training alone is not enough; therefore the training level of the learning continuum is discussed next.

4.3 Training

Simply issuing policy with no follow-up to implement that policy does not suffice; therefore, training employees is also necessary to show that a standard of due care has been taken in protecting information ("Lesson 12", 2006). Gilbert (2003) states that training builds knowledge and skills

to augment and enhance job performance and enables people to perform more effectively. Educating with training is generally for those within the organisation whose roles require special knowledge and following of specific policies and procedures for addressing information security and privacy issues and events (Herold, 2003). The author further states that training is focused on providing knowledge, skills and abilities specific to a person's job responsibilities and roles. The purpose of training is to teach people the skills that will enable them to perform their jobs more securely (NIST 800-12, 1995). Training can address many levels, from basic security practices to more advanced or specialised skills (NIST 800-12, 1995).

According to Gilbert (2003), the three distinct levels of IT security training can be tabulated as follows:

Table 4-1: Levels of IT Security Training. Source Gilbert (2003)

Level	Audience	Objective
Beginning	▪ Novice Users	▪ Provides foundation training to support performance of a specific security role.
Intermediate	▪ Security Generalists ▪ Security Specialists	▪ Used to cultivate a person by training to enhance their breadth and/or depth of security knowledge and skill.
Advanced	▪ IT Security Technicians ▪ IT Security Professionals	▪ To offer a person the opportunity to apply knowledge and skills attained through training to mission critical IT security problem-solving and technology assessment.

There is much confusion surrounding the similarities and differences between training and education. There is a need to differentiate between these two terms that are often misinterpreted in the field of information

security. Training deals with that area of learning most usually referred to as vocational (Horrocks, 2001), that is, learning practical skills to an approved level of competence. Horrocks (2001) further describes education as involving learning about the 'why' rather than merely the 'how to'. In other words, it involves the development of an understanding of why a person does what he/she does the way he/she does. Herold (2003) claims that training is a targeted, interactive event that requires the participant's full attention in order for the participant to benefit.

One organisation too many takes information security lightly. They (organisations) do not necessarily see it as part and parcel of the organisation's daily business operations. Furnell et al (2002) see the problem as one of ensuring that information security occurs both in the first instance and as an ongoing factor of an organisation's operation. An example would be when budget crises occur: a person can count on information security training and awareness being one of the first areas (if not the first area) in which the budget will be slashed (Shultz, 2004).

More often than not, managers that are responsible for overseeing information-security functions of an organisation are put under pressure by upper management to be geared up for any unforeseen changes that might occur to the organisation's budget. This change, as afore-mentioned, will result in information-security duties being compromised because of the reduced budget.

Patel (2002) believes that in any perfect-world system, the weakest link is the people using it. As one of the benefits of information-security training, employees who receive security training or who are attending security-awareness sessions will be less susceptible to social engineering and other types of attacks than before they received this training (Shultz, 2004). Practical training in IT security is of importance to learning, the feedback will help the learner to check, change and control that actions taken are adequate to existing systems (Yngström, 1996).

Although guidelines and procedures can be laid down with the strict instructions to follow them at all times, these are not likely to provide the necessary levels of security if they are not supported by a sufficient level of understanding of the motivation for them (Patel, 2002). Good security is not intrusive and can be almost invisible to typical users, who are often unaware of it or take it for granted. (Irvine et al, n.d.). It is less easy to see that, in practice, every user of the IT system in the organisation must understand the issues in IT security, not just the IT staff (Patel, 2002). The goal of training is to improve basic security practices, *not* to make everyone literate in all the jargon or philosophy of security (NIST 800-12, 1995). The importance of providing security training to the IT specialist staff is easy to see: they are the ones who must deal with the day-to-day work of ensuring that the IT systems are not compromised (Patel, 2002). However, Irvine et al (n.d.) claim that good security practice by entire user populations is a critical element of an organisation's information-assurance strategy. The following section will take a look at information-security education, and why it is crucial to organisations.

4.4 Education

Education is an advanced form of training (Gilbert, 2003). Security education is more in-depth than security training and is targeted at security professionals and those whose jobs require *expertise* in security (NIST 800-12, 1995). Education simply leverages experience in a field of study to further enhance and develop knowledge, skills and abilities (Gilbert, 2003). According to the NIST 800-12 (1995) publication, security education is normally outside the scope of most organisations' awareness and training programmes as it is more appropriately a part of employee career development. The document further states that security education is obtained through college or graduate classes, or through specialized training programmes. Because of this, most computer security

programmes focus primarily on awareness and training, as do the next few sections of this chapter.

In discussing education and training in IT security, demands to treat IT security from technical as well as organisational, legal and social points of view came forward in the beginning of the 1990s (Yngström, 1996). The Computers at Risk (1991) report stated “Security must be holistic - technology, management, and social elements; computer security does not stop or start at the computer. Security is only partly a technical problem: it has significant procedural, administrative, physical facility and personal components as well”. There are needs to understand and develop interactions between technical and non-technical parts of the total system, and the need for vehicles to support such understanding, usage, and practice including different definitions, models, criteria, paradigms, applications, and interpretations in the form of devices and safeguards for IT security (Yngström, 1996).

Although educational or awareness issues (from simply information-security guidelines to well-developed information-security education programmes) are security matters in nearly all organisations in the era of the information society, their nature is not well understood, resulting, for example, in ineffectiveness of security guidelines or programmes in practice (Siponen, 2000). Computer systems will not become more trustworthy unless a cohesive and integrated programme of information security (INFOSEC) education is established in colleges and universities (Wright, 1998). Simply passing around security guidelines in a factual manner per se, (i.e., their presentation as normal facts), as is likely to be the case in most organisations, may be an inept approach as such (Siponen, 2000).

The importance of the behavioural aspects of security is promoted while continuing to recognize the importance of technological security controls (an area which traditionally has received the greatest emphasis) (Wright, 1998). Businesses have traditionally been slow to enact strong security

measures, seeing security as an expense that adversely impacts the bottom line, rather than as an investment that contributes to the organisation's viability and competitive position in the marketplace (Wright, n.d.). Too often, managers, corporate heads, and business professionals lack fundamental knowledge about good computer security practices, are unaware of the risks to which their systems and data are exposed, and are unable to recognize and respond to security problems when they occur (Wright, 1998). Security issues affect everyone; it is not just an IT issue, it is not even just a management issue (Baker, 2001). The author further states that if a person has a user ID and password, then security is an issue that concerns that particular person. Inadequate security has left individuals and corporations more vulnerable to illegal activities such as computer fraud, telecommunications abuse, and the unauthorized disclosure, modification, or destruction of information (Wright, 1998).

Computer crime is rising and estimates of financial losses due to computer abuse range into the billions of dollars (Wright, 1998). According to Yngström (1996), prior to 1996, in schools and universities in general, there was no education in IT security and few demands for it, although these institutions were increasingly becoming heavy IT users. Both the National Institute of Justice and the National Security Agency then stated that education in the responsible design and use of computer technology was a critical part of the effort to prevent computer crime (Wright, 1998). Security in IT systems has always been of importance but it was not until the 1980s that it became an area of its own within computer science (Yngström, 1996). Yngström (1996) claims that in the 198Os, most university courses or programmes concerned with IT security were found at PhD level or in research departments. While other disciplines have well-defined bodies of educational literature, the field of computer security typically has been represented in academia by short and scattered treatments in textbooks on operating systems, data communications and databases (Wright, 1998). However, that is changing slightly as Du et al (2006) have stated that in order for the national needs for computer

security education to be addressed, many universities have incorporated computer and security courses into their undergraduate and graduate curricula. The authors articulate that in these computer-security education courses, students learn how to design, implement, analyze, test, and operate a system or a network to achieve security. In the absence of more secure computer and networked systems, the number of system disruptions, intrusions into personal privacy, and incidences that result in economic and human losses will increase (Wright, 1998). Pedagogical research has shown that effective laboratory exercises are critically important to the success of security-orientated types of courses (Du et al, 2006). However, such effective laboratories do not exist in computer-security education.

Although mundane education, training and awareness programmes may temporarily raise user interest, for many, mandatory education is considered a distracting waste of time (Irvine et al, n.d.). It is conceivable that information security education will continue being a field for specialists as few tertiary institutions offer in-depth education in this particular area. Irvine et al (n.d.) claim that a new approach is needed to convey information-security concepts that will engage the user's imagination.

4.5 Education, Training and Awareness in Healthcare

The use of ICT within healthcare establishments has been increasing at a very fast rate (Katsikas, 2000). With this growth, there needs to be a balance between securing ICT services and securing healthcare services. Although the actual interpretation of security is different within healthcare organisations than within the organisations which traditionally developed the security for IT systems (Yngström, 1996), confidentiality of data and

information is of utmost importance in healthcare, and all personnel within the healthcare environment must help to maintain it (Patel, 2002). They must be made fully aware at all times of the essential actions for this, and they must also be kept abreast of new requirements and guidelines, implying a continuing need for training (Patel, 2002). However, to concentrate IT-security issues on the discussion of privacy, and in particular within healthcare and medical systems, often leads to difficulties (Patel, 2002). Within healthcare and medical systems, there are two focuses: that of the care-giving organisation and that of the patients (Yngström, 1996). Keeping computer-stored records containing information on persons secret to all unauthorised users, and also the issue of having the correct information on persons recorded and at hand when needed are clearly problems (Patel, 2002).

It is of importance that the nature of healthcare and the nature of information security be juxtaposed in order to see where they can be integrated and be instilled in healthcare staff without compromising the nature of the two afore-mentioned aspects. There has been some initiative in this regard from the healthcare sector (to at least educate healthcare staff about some IT issues). According to IMIA (2000), the International Medical Informatics Association (IMIA) agreed on international recommendations in health informatics or medical informatics education. The IMIA recommendations centre on education needed for healthcare professionals to acquire knowledge and skills in information processing, and information and communication technology (IMIA, 2000). A three-dimensional framework was described for these educational needs. The learning outcomes were defined in terms of knowledge and practical skills for healthcare professionals in their role as: a) an IT user and, b) as an HMI (medical informatics) specialist (IMIA, 2000). However, it is important to include IT-security education within these developments in the healthcare sector, considering that in today's technological environment, especially within modern healthcare establishments, it is almost impossible for any employee to function properly without being at least security aware. It is naturally concluded that all employees of a

healthcare organisation, regardless of their function or speciality, need awareness (Katsikas, 2000).

Awareness constitutes the point-of-entry for all employees into the progression of information systems security levels (Katsikas, 2000). Training must, therefore, be provided to all types of personnel in a healthcare organisation. This training must take into account the different levels of knowledge and experience in the use and application of data protection (Patel, 2002). The challenge for security training in the healthcare environment is that IT security is a difficult topic and requires substantial background understanding of many aspects of IT in order to appreciate it. Worthwhile training in IT security must, therefore, begin by achieving a necessary level of understanding of IT before presenting the security concepts. The training curriculum in many respects can also be seen as a general IT curriculum (Patel, 2002). For the healthcare environment, the scope of the curriculum will necessarily be narrower because the objective is not to produce IT professionals, but rather to inform healthcare workers (Patel, 2002).

Security issues in healthcare environments have been subject to a number of European research projects (Patel, 2002). These security projects are important for growth with regards to security in the healthcare sector. Such projects include the likes of SEISMED, ISHTAR and MEDSEC. The SEISMED (Secure Environment for Information Security in Medicine) consortium developed extensive and detailed sets of management guidelines, technical guidelines and user guidelines (Patel, 2002). ISHTAR's (Implementing Healthcare Telematics Application in Europe) main aim was to build upon the guidelines developed within SEISMED to create a framework for implementing security in European healthcare environments (Katsikas, 2000). The ISHTAR project also aimed to produce an updated and more accessible set of guidelines, while also considering many other aspects such as legal issues, policy issues, clinical perspective and training (Patel, 2002). The MEDSEC took all the previous work from SEISMED and ISHTAR as inputs and built on it to develop a pilot training

course in the use of standards in IT security for healthcare environments (Patel, 2002).

With consideration for the importance of SETA programmes, as has been established, it is now necessary to consider the design and development thereof.

4.6 Designing and Developing a SETA Programme

The importance of security training, awareness, and education is now more than ever a priority with private and public entities alike (Gilbert, 2003). The objective of a SETA programme is to focus the attention of employees on maintaining the confidentiality, integrity and availability of information assets; it allows them to recognize IT security concerns and respond appropriately (NIST 800-50, 2003). All employees of an organisation must participate in a SETA programme, no matter which role they might fulfill. A good SETA programme highlights the importance of information security and introduces the information security policies and procedures in a simple yet effective way so that the employees of an organisation are able to understand the policies and are aware of the procedures (Kaur, 2001). Explaining what happens to an organisation, its mission, customers and employees if security fails motivates people to take security seriously (“Lesson 12”, 2006).

Federal agencies and organisations cannot protect the confidentiality, integrity and availability of information in today’s highly networked systems environment without ensuring that all people involved in using and managing IT (NIST 800-50, 2003):

- Understand their roles and responsibilities related to the organisational mission;

- Understand the organisation's IT-security policy, procedures, and practices; and
- Have at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible.

Making computer users aware of their security responsibilities and teaching them correct practices helps users change their behaviour and also supports *individual accountability*, which is one of the most important ways to improve computer security (NIST 800-12, 1995). The NIST 800-12 (1995), document further states that users cannot be truly accountable for their actions without knowing the necessary measures and how to use them.

The National Institute of Standards and Technology (NIST) is a well-recognised and internationally accepted institute responsible for developing standards and guidelines for providing adequate information security for all agency operations and assets. The NIST 800-50 (2003) document provides guidelines for building and maintaining a comprehensive awareness and training programme, as part of an organisation's IT-security programme.

The NIST 800-50 document identifies four critical steps in the life-cycle of an IT security awareness and training programme, as illustrated in Table 4-2 below:

Table 4-2: Steps of an Awareness and Training Programme. Source NIST 800-50 (2003)

Step	Objective
Programme Design	▪ An agency-wide needs assessment is conducted and a training strategy is developed and approved. ▪ Identify implementation tasks to be performed in support of established

	agency security training goals.
Material Development	▪ Focuses on available training sources, scope, content, and development of training material, including solicitation of contractor assistance if needed.
Programme Implementation	▪ Addresses effective communication and roll out of the awareness and training program. ▪ Also addresses options for delivery of awareness and training material (web-based, distance learning, video, on-site, etc.).
Post-Implementation	▪ Gives guidance on keeping the program current and monitoring its effectiveness. ▪ Effective feedback methods are described (surveys, focus groups, benchmarking, etc.).

The overall goal of this document is to facilitate the development or strengthening of a comprehensive, measurable, cost-effective IT-security programme which supports the missions of the organisation and is administered as an integral element of sound IT management and planning (NIST 800-16, 1998).

The NIST 800-50 is a companion publication to the NIST 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model.* These two documents complement each other, the NIST Special Publication 800-50 works at a higher strategic level while the NIST Special Publication 800-16 is at a lower tactical level, describing an approach to role-based IT-security training. This study will make use of the NIST 800-50 document as the basis for an awareness and training

programme. It is not the purpose of this study to carry out a full life-cycle of an information security programme. To provide a theoretical comprehension of a full SETA programme, the study will utilise the NIST 800-50 and NIST 800-16 documents and supplement them with other theoretical content. The content provided in the next few sections is merely a basic, very brief explanation of the NIST 800-16 (1998) and NIST 800-50 (2003) documents with some additions from other sources..

An articulate understanding of the three components of a SETA programme has to be formulated before the study continues to dwell on a SETA programme. The NIST 800-12 (1995) contains a comparative framework to distinguish these three components.

Table 4-3: The NIST 800-12 Comparative Framework. Source NIST 800-12 (1995)

	Awareness	**Training**	**Education**
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Teaching Method:	Media - Video - Newsletters - Posters, etc.	Practical Instruction - Lecture - Case study workshop - Hands-on practice	Theoretical Instruction - Discussion seminar - Background reading
Test Measure:	True/False Multiple Choice (identify learning)	Problem Solving (apply learning)	Essay (interpret learning)
Impact Timeframe	Short-term	Intermediate	Long-term

In the next few sections, the steps involved in the cycle of a SETA programme will be examined.

4.6.1 Designing an Awareness and Training Programme

Safeguarding information and systems, as well as other assets, requires security activity to be organized efficiently across the organisation (Guenther, 2001a). The author further states that the high-level control area covers the organisational arrangements for managing security across the organisation and the security awareness, know-how and skills of individuals with authorized access to the organisation's information, systems and other valuable assets.

Awareness and training programmes must be designed with the organisation's mission in mind (NIST 800-50, 2003). NIST 800-50 (2003) states that it is important that the awareness and training programme supports the business needs of the organisation and is relevant to the organisation's culture and IT architecture. For the programme to be successful, the users must feel that it is relevant to the subject matter and issues presented (NIST 800-50, 2003).

In the design step of an awareness and training programme, the NIST 800-50 (2003) states that the following questions should be answered:

- How to structure the awareness and training activity;
- How to (and why) conduct a needs assessment;
- How to develop an awareness and training plan;
- How to establish priorities;
- How to "set the bar" (i.e., the level of complexity of the subject matter) properly; and
- How to fund the awareness and training programme.

4.6.2 Developing an Awareness and Training Programme

According to the NIST 800-50 (2003), once the awareness and training programme has been designed, supporting material can be developed. Also, the material should be developed with the following in mind:

- **"What behaviour do we want to reinforce?"** (awareness); and
- **"What skill or skills do we want the audience to learn and apply?"** (training).

In both cases, the focus should always be on specific material that the participants should integrate into their jobs (Wilson and Hash, n.d.). In order for an awareness and training programme to be effective, awareness material should be current, interesting and the audience must not feel that the material is too general as to apply to any audience (NIST 800-50, 2003). If this happens, the users will not feel part of the programme and they will feel as if they have to do it only for the sake of doing it. The audience must feel some sense of belonging as if they are the ones who came up with the material, as if the material was specifically created for them.

As the goal of awareness material is simply to focus attention on good security practices and making all individuals aware of their commonly shared IT-security responsibilities, the awareness audience must include all users in an organisation (Wilson and Hash, n.d.). As the training material includes everything related to security that attendees need to know in order to do their jobs and is directed at a specific audience, training material is usually far more in-depth than material used in awareness campaigns or sessions (NIST 800-50, 2003).

4.7 Implementing an Awareness and Training Programme

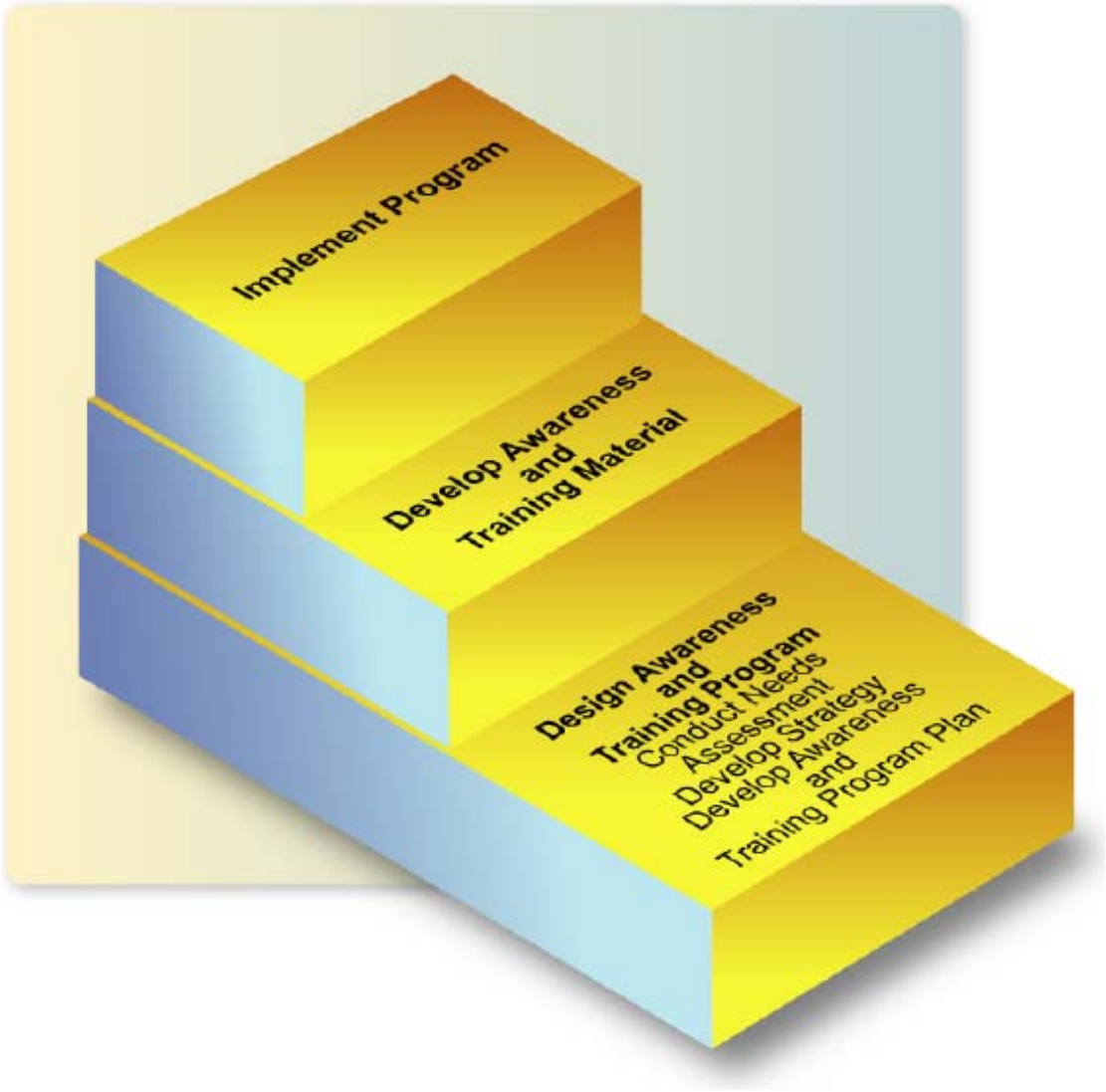
According to the NIST 800-50 (2003) publication, an IT-security awareness and training programme should be implemented only after:

- A needs assessment has been conducted;
- A strategy has been developed;
- An awareness and training programme plan for implementing that strategy has been completed; and
- Awareness and training material has been developed.

This is illustrated in Figure 4.2.

The afore-mentioned activities were mentioned in Sections 4.6.1 and 4.6.2, comprising the discussion of the design and development of a SETA programme.

Figure 4-2: Key Steps Leading to Programme Implementation. Source NIST 800-50 (2003)



The NIST 800-50 (2003) specifies that in order for the implementation of the programme to achieve support and the commitment of necessary resources, the programme must be fully explained to the organisation. This explanation is said to include expectations of agency management and staff support, as well as expected results of the programme and benefits to the organisation. The funding issues also need to be addressed. According to Wilson and Hash (n.d.), it is essential that everyone involved in the implementation of the programme understand their roles and responsibilities. The authors further state that schedules and completion requirements must also be discussed.

The implementation only begins once the plan for implementing the awareness and training programme has been explained to and accepted by agency management (NIST 800-50, 2003). Olzak (2006) asserts that employees should know what to expect. The author further states that employees should be informed of the importance of security both to the company and to each of them personally.

4.8 Post-Implementation

An organisation's IT-security awareness and training programme can quickly become obsolete if sufficient attention is not paid to: a) technology advancements, b) IT infrastructure and organisational changes, and c) shifts in organisational mission and priorities (NIST 800-50, 2003). Wilson and Hash (n.d.) state that CIOs and IT-security programme managers need to be cognizant of this potential problem and incorporate mechanisms into their strategy to ensure the programme continues to be relevant and compliant with overall objectives. Continuous improvement should always be the theme for security awareness and training initiatives, as this is one area where "*you can never do enough*" (NIST 800-50, 2003).

After the initial message delivery, it is of utmost importance to measure the effectiveness of the approach that was taken to implement the programme Olzak (2006). The NIST 800-50 (2003) suggests that the following be done to achieve this:

Monitoring Compliance: once the programme has been implemented, processes must be put in place to monitor compliance and effectiveness;

Evaluation and Feedback: various evaluation and feedback mechanisms that can be used to update the awareness and training programme plan

include surveys, evaluation forms, independent observations, status reports, interviews, focus groups, technology shifts and benchmarking;

Ongoing Improvement: this stage of the programme is focused on creating a level of security awareness and excellence that achieves a pervasive security presence in the organisation.

Managing Change: it will be necessary to ensure that the programme, as structured, continues to be updated as new technology and associated security issues emerge;

Programme Success Indicators: CIOs, programme officials, and IT-security programme managers should be primary advocates for continuous improvement and for supporting an organisation's security awareness, training and education programme.

4.9 Conclusion

The purpose of this chapter was to provide some insight into and understanding of the general SETA principles. This was done by initially providing some background on what the awareness, training and education levels of the NIST learning continuum is. The importance of information security in an organisation illustrated that modern organisations cannot do without SETA programmes. There are various obstacles that are faced by organisations in terms of securing their most valued asset, which is information. One major obstacle that was substantiated is that of human beings continuing to be a threat within their organisations. This predicament can, however, be dealt with by instilling a security-awareness culture within an organisation.

The chapter ended off by providing a brief summary of designing, developing and implementing a SETA programme, using the NIST 800-16 and NIST 800-50 as primary sources. With this gained understanding of

security education, training and awareness programmes and the importance thereof, the stage is now set for the discussion of a role-based SETA programme for the South African healthcare environment in Chapter 5.

Chapter 5

A Role-Based SETA Model for the South African Healthcare Environment

This chapter presents a Role-Based SETA Model for the South African Healthcare Environment. It further provides an overview of the various steps that comprise the model.

"If I only had one dollar to spend on information security, I'd spend it on awareness training". ***– Shawn Lukaschuk (2001) –***

"*'The methods that will most effectively minimize the ability of intruders to compromise information security are comprehensive user training and education. Enacting policies and procedures simply won't suffice. Even with oversight the policies and procedures may not be effective: my access to Motorola, Nokia, ATT, Sun depended upon the willingness of people to bypass policies and procedures that were in place for years before I compromised them successfully."* ***– Kevin Mitnick -***

5.1 Introduction

South Africa hosts more than forty million citizens. She has one of the strongest economies in Africa; however, the country of South Africa has a new democracy. Naturally, with every new endeavour, there are new challenges. One of the departments of the South African government that is faced with many obstacles is the National Department of Health. In addition to issues such as lack of adequate infrastructure, insufficient funding (especially in the public healthcare sector), corruption and the shortage of healthcare staff; the issue of information security is of growing concern. The necessity of information security is brought upon the healthcare sector because the healthcare sector deals with extremely sensitive information. There are various controls or countermeasures that the healthcare sector can use to protect this information, with Information Security Education Training and Awareness being one of them. It is a very important control as can be gathered from Kevin Mitnick's quote at the start of the chapter.

Since the South African health sector is faced with the afore-mentioned obstacles at a primitive or “basic needs” level (e.g. infrastructure), it is very difficult to pay special attention to information security as the groundwork has not been properly done after more than ten years of democracy. It is conceivable that some stakeholders may feel that whilst the National Department of Health is still at a developing stage in order to serve the population adequately from a healthcare perspective, information security is one of the last things to be apprehensive about. The importance thereof, cannot however, be negated. For this reason, this chapter presents the Role-Based SETA Model (RB-SETAM) as a comprehensive approach to addressing SETA in the healthcare environment. The model is introduced in Section 5.2 with a more detailed discussion of each phase of the model following from Section 5.3 onwards.

5.2 Overview of the RB-SETA Model

The Role-Based SETA Model (RB-SETAM) is proposed as a primary output of this research (refer to Figure 5.1, inserted as a fold-out page at the end of Chapter 5, to facilitate easy reading while referring to the model diagram). The crux of the model is about ensuring that employees in the healthcare environment know enough, do enough and feel good enough (have a positive mind-set) with regard to information security to contribute significantly to the protection of healthcare information. This is achieved through the development of a SETA programme which addresses Education Training and Awareness (ETA) in a particular combination unique to each role in the healthcare environment. The following principles form the basis of the model:

- A role-based approach is followed, to allow the creation of a SETA programme which is customized for each role in the healthcare environment;

- A unique combination of education, training and awareness (ETA) requirements is identified and captured as the “ETA Mix” for each role. The ETA Mix ensures that the three levels of the learning continuum are addressed adequately and uniquely for each role;

The model is divided into three phases that are comprised of the following steps:

Phase 1

- Identify Employees (Step 1.1)
    - The employees that are employed in the establishment are identified;

- Develop Roles (Step 1.2)
    - Roles that contribute to the organisation meeting its objectives, are developed;

- Map Employees to Roles (Step 1.3)
    - Employees that meet the requirements of a developed role or more than one role, are mapped to or associated with the role(s);

- Determine ETA Mix for Each Role (Step 1.4)
    - The security education, training and awareness requirements are determined for each role and captured as the ETA Mix;

Phase 2

- Design SETA Programme to Satisfy ETA Mix (Step 2.1)
    - A SETA programme is designed according to the needs of each role, based on the captured ETA Mix;

- Develop SETA Programme to Satisfy ETA Mix (Step 2.2)
    - A SETA programme is developed according to the design done in Step 2.1;

Phase 3

- Run the SETA Programme (Step 3.1)
    - The developed SETA programme is implemented for all the roles across various departments in the organisation;

- Measure ETA Level (Step 3.2)
    - The success of the SETA programme is determined through measuring the knowledge, behaviour and attitude of employees about and towards information security;

- Assessment of the ETA Level (Step 3.3)
    - The measured ETA level is assessed as to whether, it is acceptable or not;

- Change the SETA Programme (Step 3.4)
    - The SETA programme is analysed as to whether it must be modified or not, based on the outcome of the measurement of the employees' ETA level;

- Change of ETA Mix and/or Roles (3.5)
    - The ETA mix of each role and/or the role-determining characteristics of each role are scrutinised to establish whether they must change.

The following sections will now discuss each of these steps in more detail.

5.3 Identify Employees (Step 1.1)

Finding the best possible people who can fit within an organisation's culture and contribute to the organization is a challenge and an opportunity ("Recruiting", 2007). Whether an employee is well suited to the job depends, in part, on whether he or she is capable of performing the job's

essential functions (Commonwealth of Pennsylvania, n.d.). Employees will be identified to work for a particular organisation based on the required skills and knowledge that they posses. The model assumes that the Human Resources (HR) Department of the healthcare establishment, being involved in the recruitment of employees, will be in a position to provide a list or database of employees who are employed and also provide updated information, such as details of newly appointed employees and employees who have resigned. These employees are assigned to various roles (in Step 1.3), based on the requirements of the employees' jobs.

5.4 Develop Roles (Step 1.2)

The word **role** has been in existence for a long time in the English language. "A role is defined as a part played by an actor or other", or, simply put, "a function" ("Definition of a role", 1949). This is an ancient definition of the word *role*, as can be found in the Chambers' Etymological English Dictionary. The modern-day definition of the word *role* can be found in an online dictionary. "A role is a part or character played by an actor or actress" ("Role", 2007). The definition, not surprisingly, remains the same, but is now gender sensitive. In relation to the healthcare environment, the role (part or character) will be performed by an employee such as a doctor or a nurse.

The NIST 800-16 (1998) defines roles and responsibilities as functions performed by someone in a specific situation and obligations to tasks or duties for which that person is accountable. It further declares that a role-based approach assumes that a person will take on different roles, over time, within an organization and have different responsibilities in relation to IT systems.

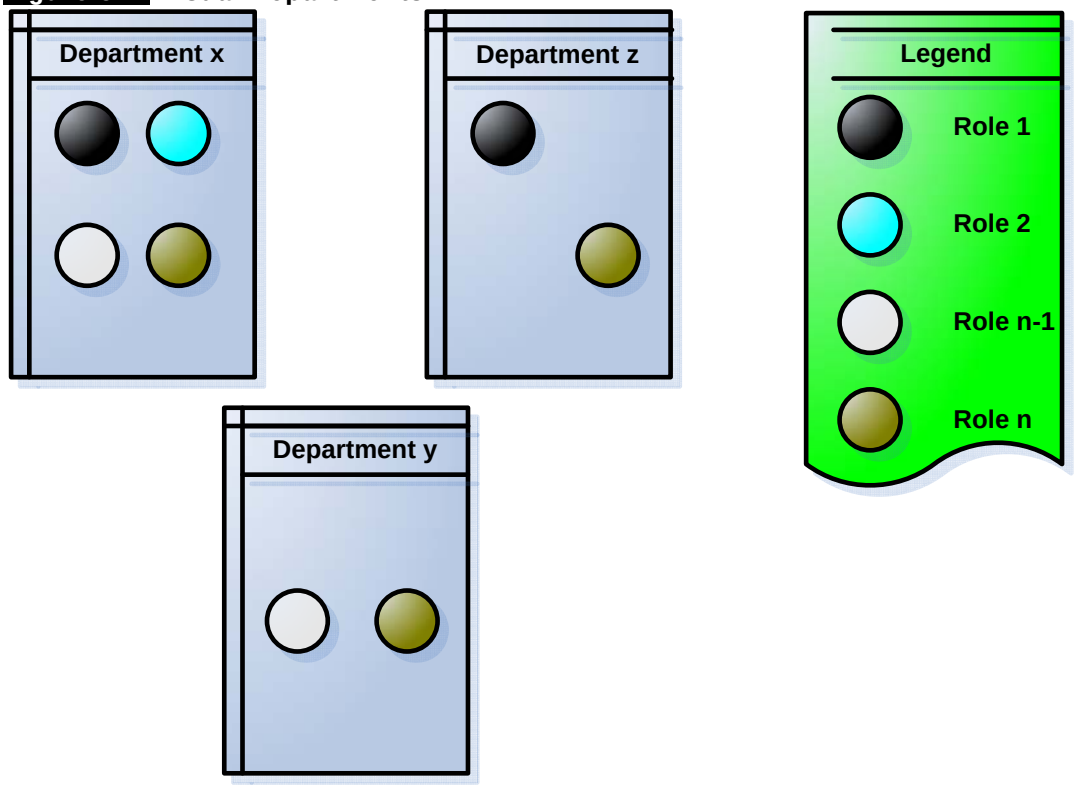
Role-based approaches are commonly used in the application of role-based access controls (RBAC). This is a centrally administered approach

with authorisation decisions based on the roles individuals have within the organisation (Stenbakk and Oie, 2004).

In the healthcare environment, people employed at a particular healthcare organisation are assigned to roles. These employees must then “play their parts” which will ensure that the healthcare organisation achieves its objectives.

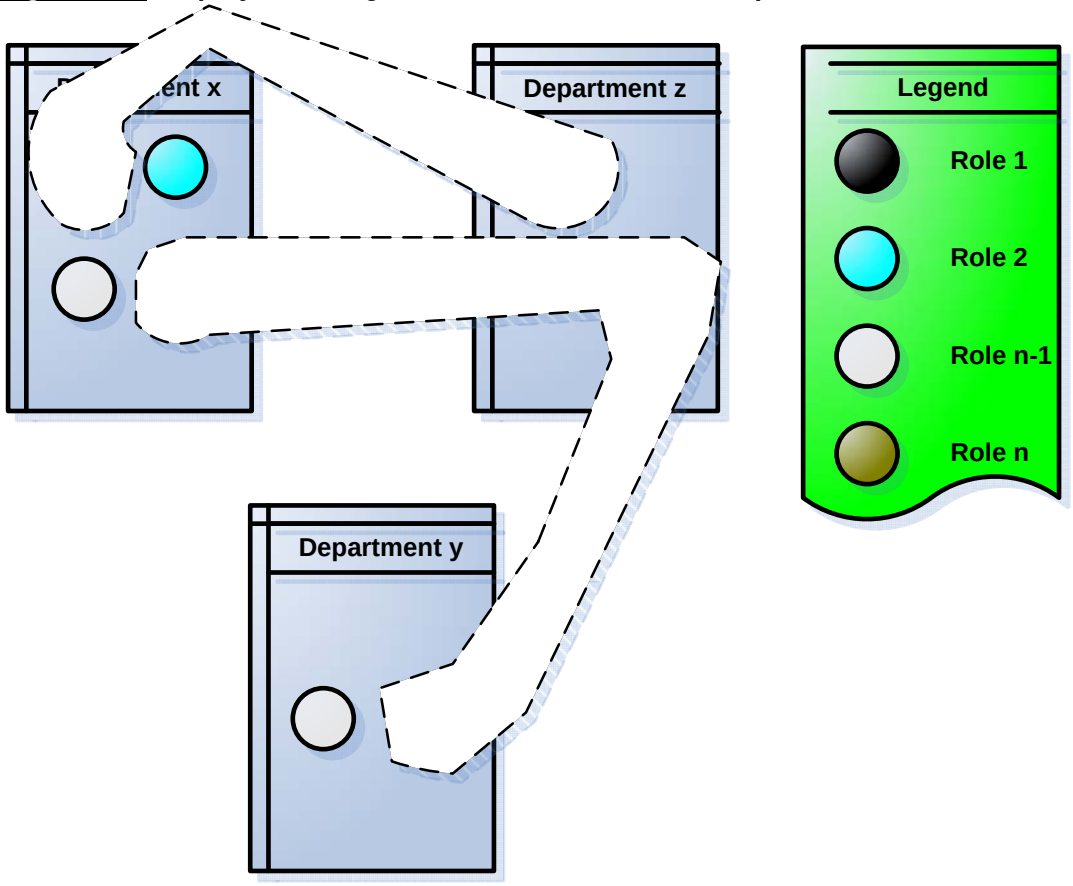
A typical healthcare organisation consists of various departments. A particular role can be found in more than one department. Figure 5.2 depicts various departments with different roles being available in multiple departments.

Figure 5.2: Visual Departments



Each colour represents a particular role. The presence of a colour in all departments means that a role can be found across all the departments. In this example, *role n* can be found across all the departments. An example of a role found in only one department, is *role 2*. Figure 5.3 better depicts the occurrence of roles across various departments.

Figure 5.3: Employees Assigned to Roles in Different Departments



In Step 1.2 of the model, all roles must be identified at the healthcare organisation as well as the function(s) of each role. The NIST 800-50 (2003) requires that, as a minimum, the following roles (which are further divided into sub roles) should be addressed:

- Executive Management;
- Security Personnel;
- System Owners;
- System Administrators and IT Support Personnel;
- Operational Managers and System Users.

Table 5-1 illustrates an example of departments and roles that can be found at a healthcare organisation. These reside in the afore-mentioned "system user" category.

Table 5-1: Example of Departments and Roles at a Healthcare Organisation. Source "Health Care" (2005)

Department	Role(s)
Radiography	▪ Nurse ▪ Surgeon ▪ Physical Therapist ▪ Podiatrist
Intensive Care Unit	▪ Doctor ▪ Nurse ▪ Physical Therapist
Maternity	▪ Doctor ▪ Nurse
Emergency	▪ Surgeon ▪ Nurse

The objective of this section was to identify roles that can be found at a particular healthcare organisation and how some roles can exist across various departments at a healthcare organisation. The next section will demonstrate how an employee is mapped to a role.

5.5 Map Employees to Roles (Step 1.3)

Role activation involves the mapping of a user (or employee) to one or possibly many roles, and a particular role for a user can be activated if the user is authorised for the role being proposed for activation (Stenbakk and Oie, 2004).

Figure 5.4 shows an M:1 relationship between various employees and a role, showing that multiple employees can be mapped to one role.

Figure 5.4: Mapping of Employees to a Role (M:1)

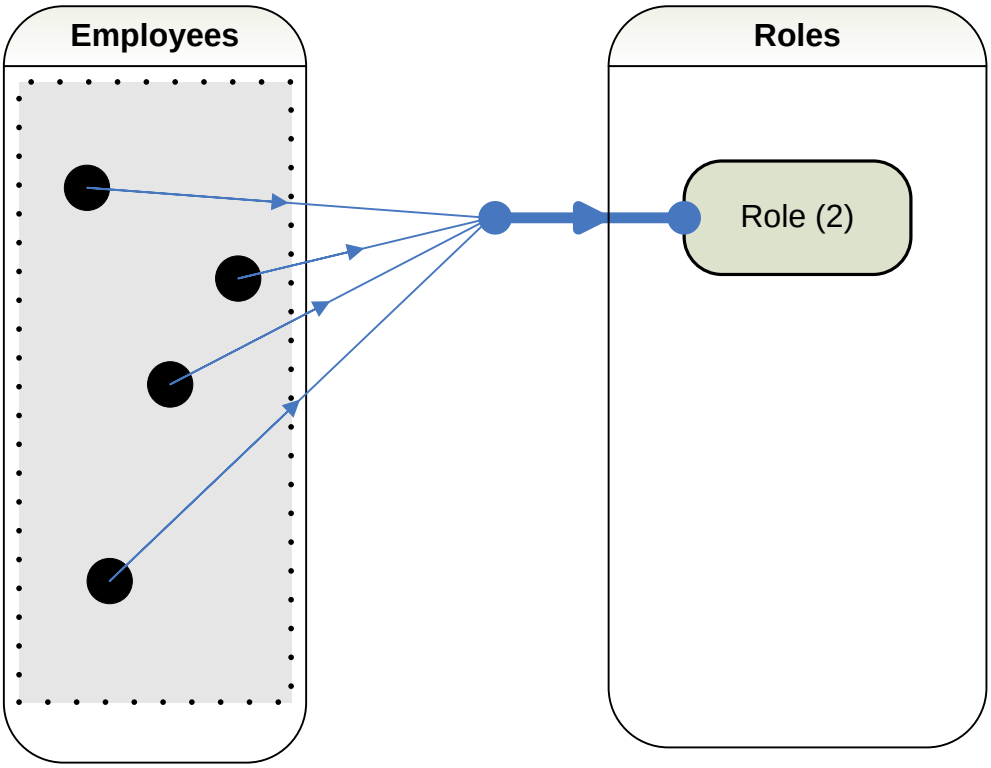
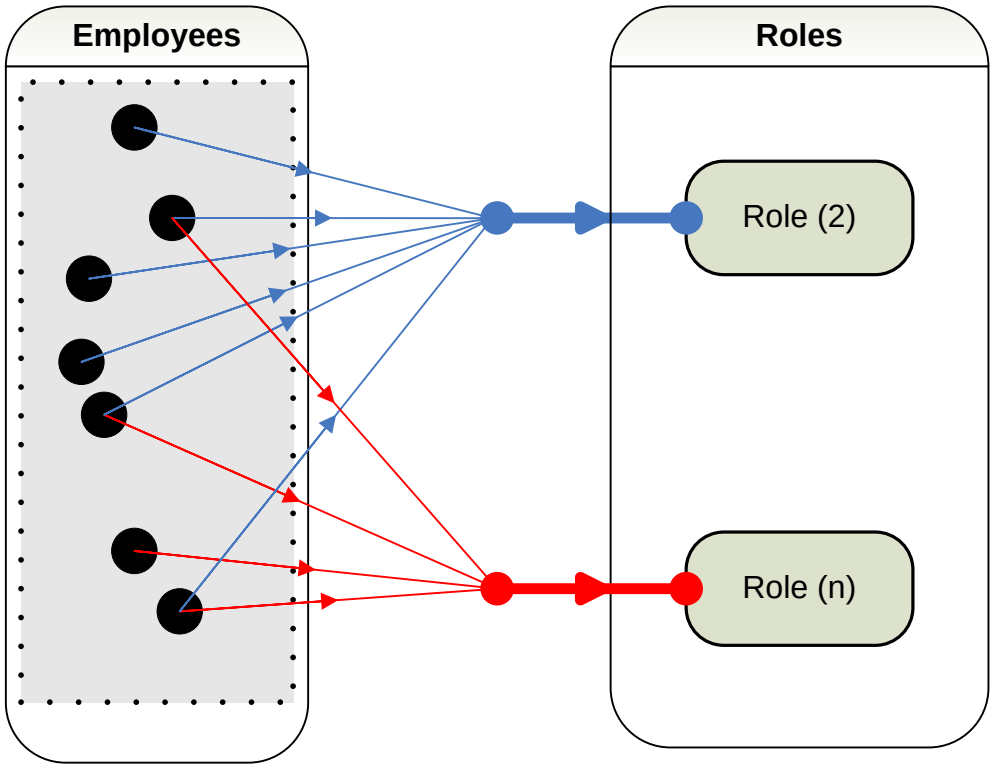


Figure 5.5 illustrates an M:N relationship between roles and employees, showing that multiple employees can be mapped to one role and that one employee can be mapped to multiple roles.

Figure 5.5: Mapping of Employees to Roles (M:N)



At the conclusion of Step 1.3 (Map Employees to Roles), the focus shifts to the determination of the ETA Mix which is required for each role.

5.6 Determine ETA Mix for Each Role (Step 1.4)

Security, Education, Training and Awareness (SETA) is well known in Information Security. Employees using information technology need to be aware of the kinds of risks that are associated with the use of IT and how to ensure that these risks do not compromise the organization because of their actions (whether intentional or not). A SETA programme will assist in aiding employees throughout organisations to be more knowledgeable and aware of, and be skilled in the handling of security issues that involve any organisation's most valued asset, information.

A SETA programme is typically run throughout the various departments of an organisation. Based on the needs of that particular organisation, an organisation will choose whether to run a fully fledged SETA programme throughout or just to consider one of the learning levels (Education, Training and Awareness) that are contained within the SETA learning continuum as discussed in Section 4.7 of the previous chapter.

This research proposes a more focused approach to defining an Education, Training and Awareness Mix (**ETA Mix**) which is unique to the role that an employee fulfils.

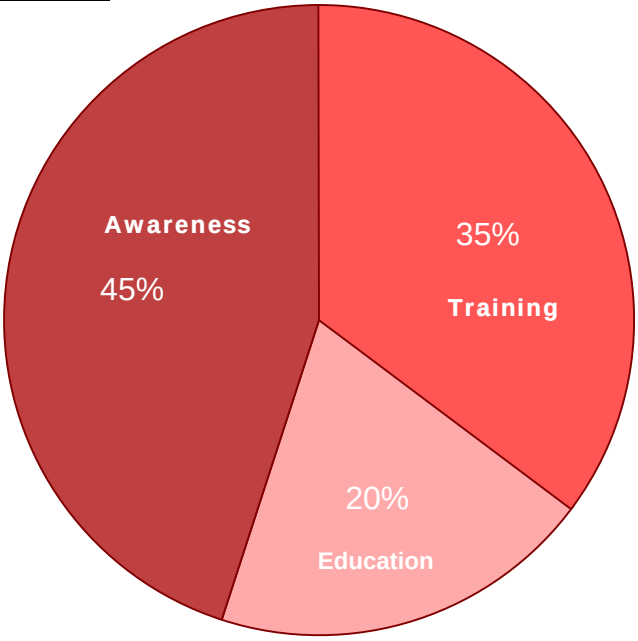
5.6.1 What is the ETA Mix?

The concept of the **ETA Mix** is based on **education**, **training** and **awareness**. The **ETA Mix** ensures that each role (based on the three levels of the learning continuum) is segregated from any other role in terms of the issues that need to be addressed in information security education, training and awareness. This study therefore sees the **ETA Mix** as:

- The required level of awareness necessary to ensure that an employee associated with a particular role will be able to perform their tasks with an acceptable attitude;
- The required level of training necessary to ensure that an employee associated with a particular role will be able to perform their tasks with acceptable behaviour; and
- The required level of education necessary to ensure that an employee associated with a particular role will be able to perform their tasks with acceptable knowledge.

An ETA mix is defined for each identified role. An example is depicted in Figure 5.6.

Figure 5.6: ETA Mix for the Role of Doctor



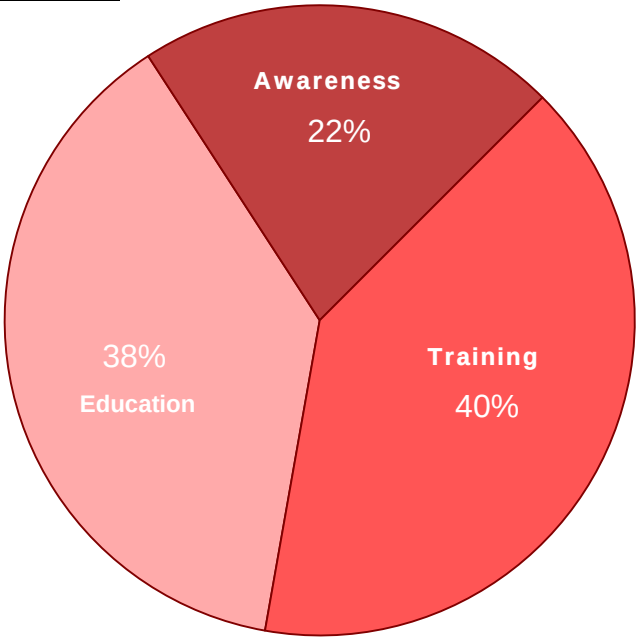
5.6.2 Why the ETA Mix?

The objective of the **ETA Mix** is to determine the requirements for information security regarding:

a) the mind-set (awareness);
b) skills or behaviour (training); and
c) knowledge (education).

These must be determined for each role, the question being how much emphasis must be placed on the ETA components, i.e., whether the requirements can be met through education, training and/or awareness. As the proposed model focuses on a role-based approach, each role will therefore need a different ETA Mix to the other roles. A typical change to this ETA Mix is then reflected in Figure 5.7 below.

Figure 5.7: ETA Mix for an IT Specialist



A role-based approach ensures that for each role, each component of the learning continuum proposed in the NIST model (NIST 800-16, 1998), receives adequate emphasis.

An example is now presented to illustrate the necessity of differentiated ETA Mixes. For simplicity, only one role is associated with the employees used in the example.

Assume that at a hospital, for the roles of doctor and secretary, the following applies:
a) a doctor's and a secretary's usage of a computer on a daily basis varies, and
b) the kind of IT systems and data that they have access to varies.

Table 5-2 encompasses a fictional scenario at a particular hospital.

Table 5-2: Scenario Description

Scenario:
Lavela is a doctor and Owam is an administrative secretary. Lavela will come to the hospital, not daily, to see his clients. Owam on the other hand sits at the reception welcoming new patients and the old ones whilst

capturing and updating the required information.

Based on this scenario, Owam is bound to access different data as compared to Lavela. She will have access to things like the account information and medical aid information of the patient. Lavela will have access to the protected health information of his patients, only. On the other hand, Owam will be able to access information of any patient that has visited the hospital (assuming that such a policy is applied by the hospital).

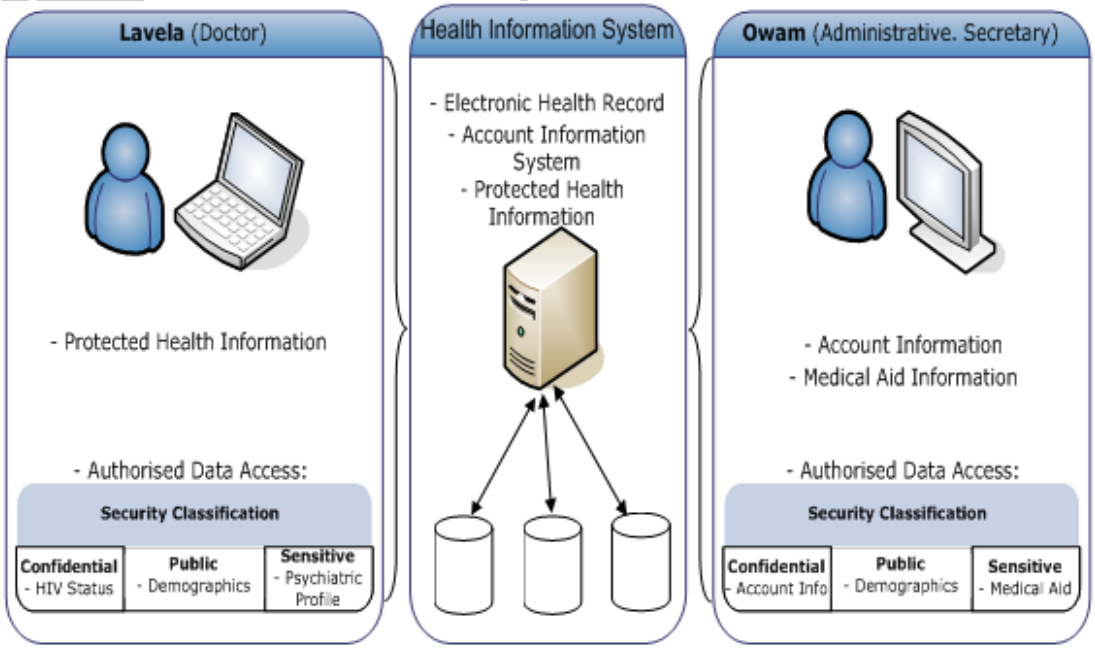
It is conceivable that these two users will require different kinds of information security training, awareness and education. Owam may require the inclusion of awareness and training in a SETA programme developed for administrative secretaries, with no education component. Lavela on the other hand, may require a substantial education component which addresses (inter alia) standards in healthcare and the role thereof in contributing to better information security. This may not be required for administrative secretaries.

Thus, the ETA Mix per role is differentiated based on the kind of work that employees perform (i.e. the roles that are assigned to them) and the IT systems and data they access as part of doing their job.

5.6.3 Determining the ETA Mix for Each Role

Continuing with the scenario provided in Table 5-2, Figure 5.8 provides more detailed information about the systems and data that Lavela and Owam access to do their jobs.

Figure 5.8: Scenario of Access According to Roles



From the scenario, it is evident that the systems and data that employees in different roles access, are not the same.

The RB-SETA model proposes that the ETA Mix be determined through the composition of an ETA profile for each role. As each role will have its own requirements in terms of the acceptable behaviour (training), attitude (awareness) and knowledge (education) about information security at a healthcare organisation, the necessary stakeholders must be involved to determine these requirements. The ETA requirements will be captured in the ETA profile and the ETA Mix calculated based on this.

Assuming that the ETA requirements for Lavela and Owam have been determined, an example of what the ETA profile for their roles would look like is presented in Figure 5.9 and Figure 5.10.

Figure 5.9: Example of a Profile for the Role of a Doctor

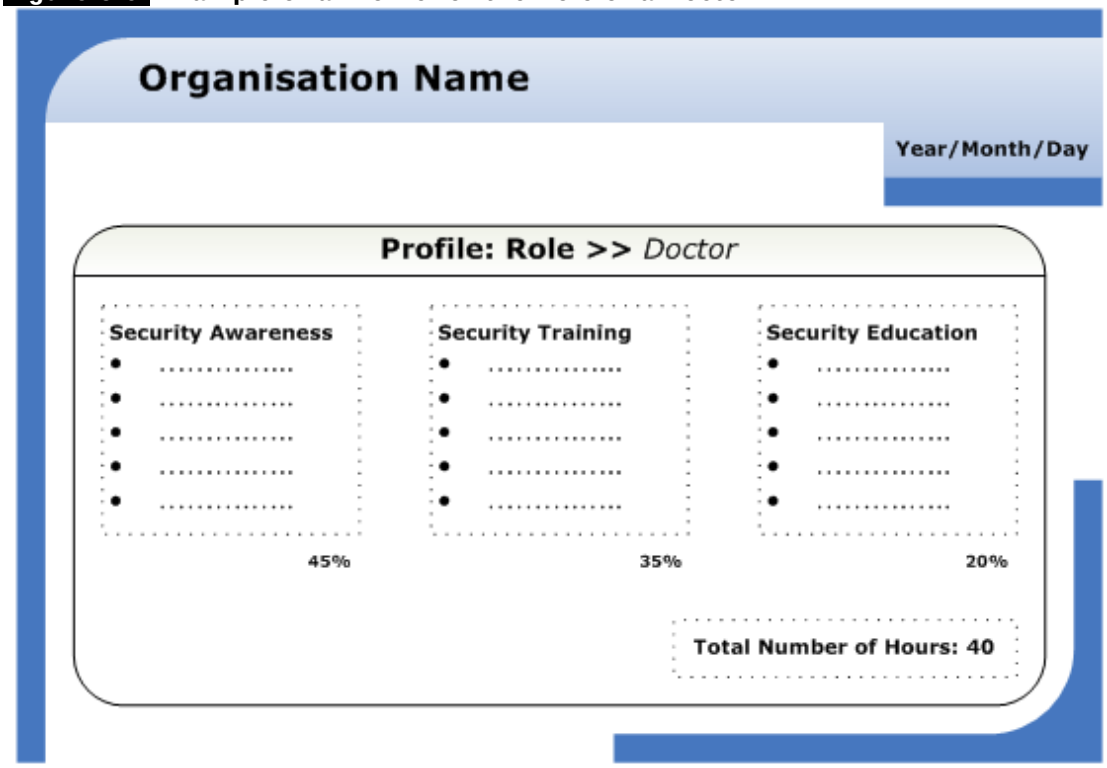


Figure 5.10: Example of a Profile for the Role of an Administrative Secretary

It is outside of the scope of this research to determine exactly who the stakeholders are and what the mechanisms will be to determine the ETA Mix for each role. However, since it is analogous to the needs assessment phase of the development of training and awareness programmes, the following suggestions from the NIST SP 800-50 for stakeholders and mechanisms to determine IT security awareness and training needs, can be adopted (NIST 800-50, 2003, p. 17):

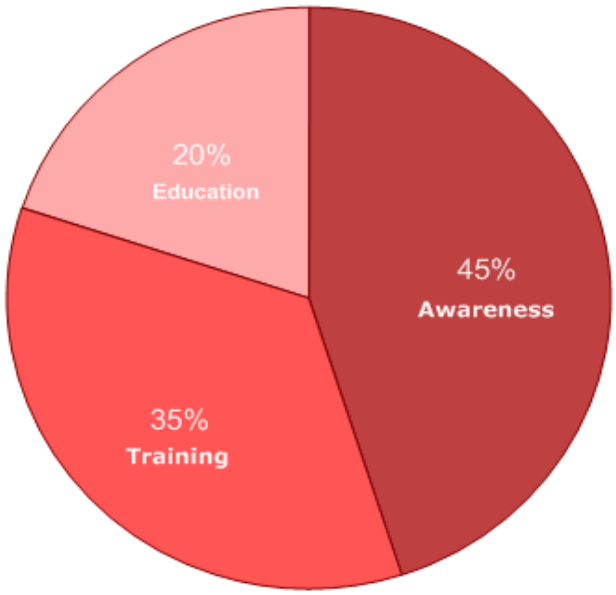
- Interviews with all key groups and organisations identified;
- Organisational surveys;
- Review and assessment of available resource material, such as current awareness and training material, training schedules, and lists of attendees;
- Analysis of metrics related to awareness and training (e.g., percentage of users completing required awareness session or exposure, percentage of users with significant security responsibilities who have been trained in role-specific material);
- Review of security plans for general support systems and major applications to identify system and application owners and appointed security representatives;
- Review of system inventory and application user ID databases to determine all who have access;
- Review of any findings and/or recommendations from oversight bodies (e.g., Congressional inquiry, inspector general, internal review/audit, and internal controls programme) or programme reviews regarding the IT security programme;
- Conversations and interviews with management, owners of general support systems and major applications, and other organisation staff whose business functions rely on IT;
- Analysis of events (such as denial of service attacks, website defacements, hijacking of systems used in subsequent attacks,

successful virus attacks) might indicate the need for training (or additional training) of specific groups of people;

- Review when technical or infrastructure changes are made;
- The study of trends first identified in industry, academic, or government publications or by training/education organisations. The use of these "early warning systems" can provide insight into an issue within the organisation that has yet to be seen as a problem.

As shown in Figure 5.9 and Figure 5.10, the ETA profile will contain a list of the required education and training programmes for each role together with focus areas, which are of importance in an awareness programme for the role. The total number of hours for each type of programme is shown as a percentage of the total number of hours in the SETA programme required for the role. This therefore represents the ETA Mix for the role. For example, for Lavela, 45% is required for awareness, 35% for training, 20% for education; and the pie chart making up the ETA Mix for the role can be depicted as in Figure 5.11.

Figure 5.11: Example ETA Mix for Lavela's Role



Once the ETA profile and ETA Mix have been determined for each role, the SETA programme must be designed to satisfy these requirements. This sees the model reaching phase 2 of the RB-SETAM cycle.

5.7 Designing, Developing and Implementing a SETA Programme (Steps 2.1, 2.2 and 3.1)

Phase 2 of the model starts off with the SETA programme being designed for every role in the organisation. This becomes Step 2.1 of the model. Step 2.2 of the model deals with developing a SETA programme for every role in the organisation. The designing and developing of a SETA programme have been discussed in Chapter 4 of this study. The discussions can be found in Sections 4.6.1 and 4.6.2.

After a SETA programme has been designed and developed, it has to be implemented across the organisation. The implementation of a SETA programme sees the model reaching Phase 3 of the model. Step 3.1 deals with the implementation of a SETA programme for the roles. The factors of importance in the implementation of a SETA programme were discussed previously, in Section 4.7 of this study.

5.8 Measure ETA Level (Step 3.2)

After a SETA Programme has been implemented, the Education Training and Awareness (ETA) level of the employees needs to be measured in order to ensure that the programme was effective enough. The next section of this study will further investigate why this is necessary. The study will then briefly discuss who might be the responsible stakeholder(s) to monitor this level amongst the employees and what must be measured. It is, however, not the purpose of this study to address the aspect of measuring the ETA level in detail.

5.8.1 Why is the ETA Level Measured?

The NIST 800-50 (2003) states that you can never do enough when it comes to security, and that after a SETA programme implementation, it is necessary to:

- Monitor compliance;
- Evaluate and receive feedback;
- Manage change;
- Raise the bar (ongoing improvement); and
- Have programme success indicators.

Step 3.2 (measuring the ETA level) relates to monitoring compliance, receiving and evaluating feedback and programme success indicators. The management of change and ongoing improvement, is handled in Step 3.4 (revising the SETA programme).

Upon the completion of a SETA programme, it should be verified whether it did, in fact, meet the needs of the employee that underwent the programme, and the needs of the organisation offering the programme. This will help in ensuring that the programme is meaningful and adds value to both employees and the organisation.

The main reason why the ETA level is measured is to determine if the SETA programme was successful. Organisations can have different objectives when it comes to the outcomes of a SETA programme. This, in turn, will determine what an organisation considers as ‘successful’ after a SETA programme has been implemented. According to the NIST 800-16 (1998), measures of success should be derived from the individual’s normal work products rather than from classroom testing. This directly ties the individual’s performance to its impact on the organisation’s mission (NIST 800-16, 1998). This can be achieved by evaluating education, training and awareness levels of employees that underwent the SETA programme and measuring these outcomes against certain

benchmarks that have been set by the organisation. These benchmarks will serve as the level of success for the intended objectives of the SETA programme.

5.8.2 Who is Responsible?

In order to ensure that a SETA programme is conducted in line with the requirements of the organisation, there must be relevant stakeholders appointed by the organisation to monitor the whole process. Supervisors with acceptable attributes in the field of information security can be appointed to monitor employees undergoing a SETA programme. These supervisors (or line managers) will work hand-in-hand with an evaluator that is experienced in the measurement of the effectiveness of (S)ETA programmes.

5.8.3 What is Measured?

As has been mentioned previously, it is not within the scope of this study to analyse the measurement of the ETA level in detail.

The NIST 800-16 (1998) recommends that an evaluation process should produce four types of measurement:

- First, evaluation should yield information to assist the employees themselves in assessing their subsequent on-the-job performance;
- Second, evaluation should yield information to assist the employees' supervisors in assessing individual students' subsequent on-the-job performance;
- Third, it should produce trend data to assist trainers in improving both learning and teaching;
- Finally, it should produce return-on-investment statistics to enable responsible officials to allocate limited resources in a thoughtful, strategic manner among the spectrum of IT security awareness, security literacy, training, and education options for optimal results among the workforce as a whole.

The evaluation process is a complex one which requires proper planning and the development of an accompanying evaluation plan.

5.9 Assessment of the ETA Level (Step 3.3)

Step 3.3 represents the simple decision of whether the ETA level is acceptable or not. This will be based on the measurement of the ETA level that occurred in the afore-discussed Step 3.2. If the ETA level does meet the requirements as set per the benchmark for each employee (individual), role (aggregate or average per role) and the healthcare establishment as a whole, the employees are considered as being in the right state of mind, possessing the necessary skills and having enough knowledge for them to perform their duties in the context of their roles. This would then imply that the RB-SETA model has reached the end of its cycle; however, it must be noted that it is **theoretically not possible** for the model to be at this **end** state. This is purely due to the fact that an organisation will experience a certain staff turnover due to employees resigning and new ones being appointed. Other organizational changes, such as moving employees between departments, will further trigger the continuous running of the SETA programme.

The next section (Step 3.4) discusses what will happen if the assessed ETA level does not meet the requirements that have been set.

5.10 Change the SETA Programme (Step 3.4)

From time to time to time, it is necessary to review the SETA programme that the organisation has been compelling its employees to undertake. In particular, at the post-implementation phase, it is necessary to manage changes and have ongoing improvement. The relevant stakeholders might

feel that there is a need to revise the SETA programme. The stakeholders might need to change the SETA programme based on the following scenarios, but not limited to them:

- They might feel that it was not effective enough;
- They might feel that some of the objectives were not accomplished; or
- They might simply feel that it was not appealing to employees.

There are many reasons that can contribute to an occurrence of these scenarios. This study recognizes two reasons that will require the SETA programme to be altered.

The first reason is that the employees might not have performed well enough to satisfy the desired results that were expected by the stakeholders. The stakeholders might feel that the SETA programme did not impact on those employees that did not meet the expectations well enough. This will then lead the stakeholders into believing that these employees might need to repeat some courses, or courses must be offered in different formats.

The second reason is because an organisation might experience technology changes or organisational changes, or perhaps there might be new requirements for employees to perform their duties in a secure manner. The NIST 800-50 (2003) states that an organisation's SETA programme can quickly become obsolete if insufficient attention is paid to technology advancements, IT infrastructure and organisational changes, and shifts in organisational mission and priorities. It is recommended that the relevant stakeholders (e.g. Line Managers and CIOs) be cognisant of this potential reason and incorporate mechanisms to ensure that the programme does continue to be relevant and compliant with overall objectives, as stated in Section 4.8.

In Step3.4, if the decision is that the SETA programme must not change, it is necessary to investigate one (or both) of the following two:

- Whether the ETA Mix for a particular role must change or not; and/or
- Whether the requirements for a particular role must change or not.

These decisions are made in Step 3.5, which is discussed in the next section.

5.11 Change the ETA Mix and/or Roles (Step 3.5)

Step 3.5 comprises the last step of Phase 3 of the RB-SETA model. In this section, the necessity of revising roles, the ETA Mix and the ETA profile per role, will be discussed.

As was previously mentioned in Section 5.10, at the post-implementation phase of a SETA programme it is necessary to manage changes and have ongoing improvement. This is true for the SETA programme developed for all roles in organisations. Each role has its own set of requirements in order for employees to perform their security-related tasks appropriately. However, security requirements to protect an organisation's most valued asset, information, might change. Training needs are shifted as new skills and capabilities become necessary to respond to new architectural and technology changes (NIST 800-50, 2003). Therefore, the ETA Mix and profile for the affected roles within the organisation must be adapted accordingly by the stakeholders. This will be done by shifting the intensity towards one of the three elements of the ETA Mix (education, training or awareness) and minimising the focus from one, or both of the remaining two components. These changes must be carried through to the design and development steps of the SETA programme.

In terms of ongoing improvement, the stakeholders concerned must conduct research into new technologies and good practices necessary for the roles, and integrate these into the SETA programme of an

organisation. This will be done similarly by first adapting the ETA mix and profile of each affected role and then redesigning and re-developing the SETA programme. If there is no need to alter the ETA Mix and/or roles then the SETA programme can continue running in its current format.

The success of a SETA programme is a determining factor in ensuring that a change in an organisation occurs that will see everyone willing and being capable of performing their security-related tasks. Through this change, security incidents will decline and top management will see that there is a tangible return-on-investment on the organisation's SETA programme.

5.12 Conclusion

One of the measures that can be utilised to protect healthcare information is a SETA programme. This chapter has proposed a role-based SETA model for the South African healthcare environment. The model consists of various phases comprised by various steps within them. In Phase 1 which is the initial phase, the main steps are: a) identifying employees, b) developing roles, c) mapping employees to roles, and d) determining the ETA Mix.

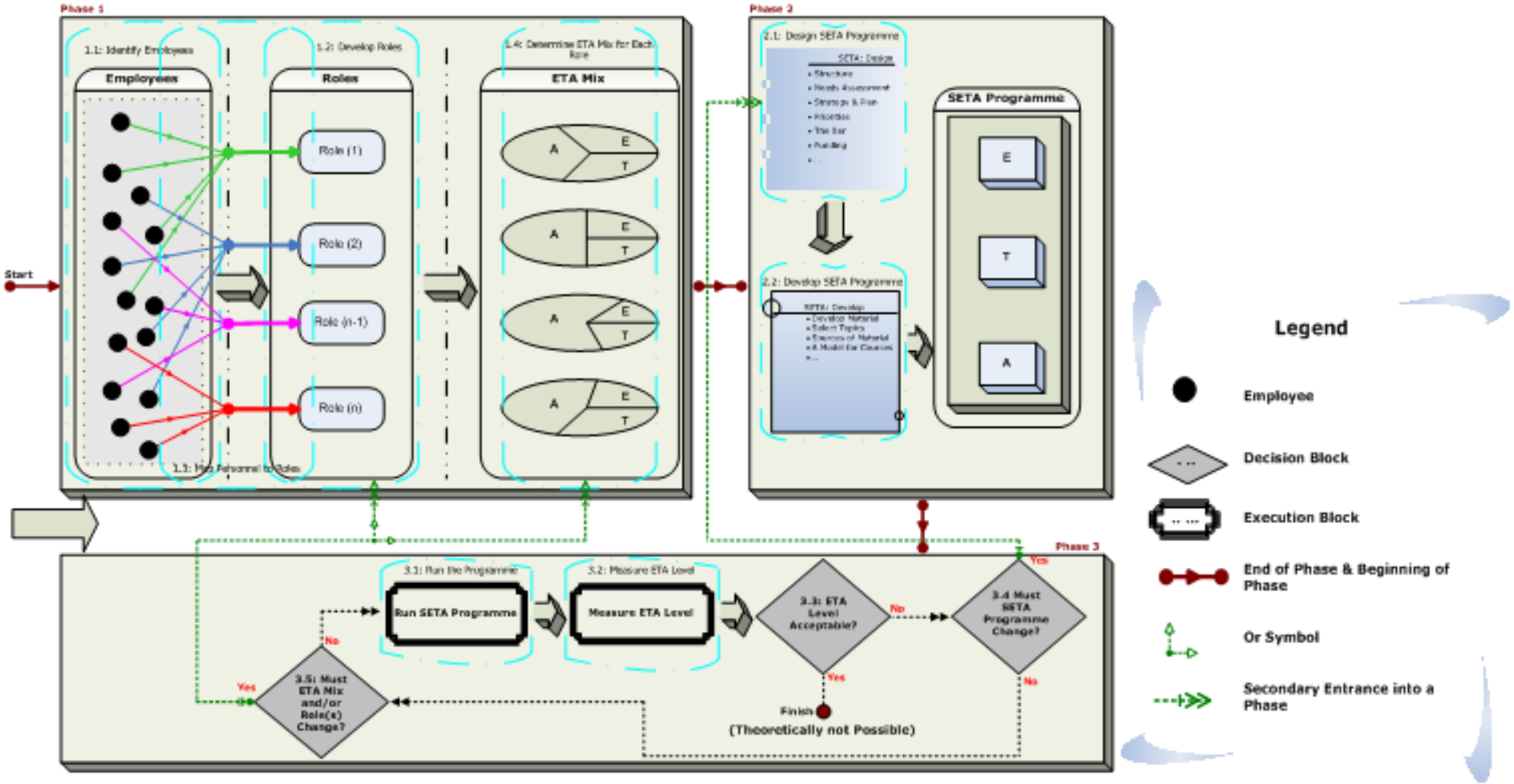
Phase 2 consists of steps that deal with the traditional SETA programme activities, viz.: a) designing a SETA programme, and b) developing a SETA programme.

Phase 3 of the role-based SETA model for the South African healthcare environment is comprised by five steps, being: a) running the SETA programme, b) measuring the ETA level, c) assessing whether the ETA level is acceptable, d) querying if the SETA programme must change, and d) determining whether the ETA Mix and/or roles must change.

The core output of this research is the proposed RB-SETA model, which in particular uses the ETA Mix mechanism to ensure that each role in the healthcare organization addresses education training and awareness in a

focused combination, unique to each role. The ETA Mix is derived from an ETA profile that is generated for a particular role. The ETA Mix ensures that each role's ETA requirements have been addressed sufficiently by customising the ETA dimensions of each role. The ETA Mix can be useful in ensuring that a SETA programme implemented by a healthcare organisation, is effectual.

Figure 5.1: RB-SETA Model



Chapter 6

Conclusion

In Chapter 5, a role-based SETA model (RB-SETAM) for the South African healthcare environment was proposed. The model helps in ensuring that healthcare employees are able to perform the security- and privacy-related functions required by their roles, adequately.

In this chapter, the research presented in this dissertation is concluded. Chapter 6 provides an overview of how the objectives of the research were met throughout the dissertation. The benefits of the RB-SETA model are discussed and some areas suitable for future research are suggested.

"Who could deny that privacy is a jewel? It has always been the mark of privilege, the distinguishing feature of a truly urbane culture. Out of the cave, the tribal teepee, the pueblo, the community fortress, man emerged to build himself a house of his own with a shelter in it for himself and his diversions. Every age has seen it so. The poor might have to huddle together in cities for need's sake, and the frontiersman cling to his neighbors for the sake of protection. But in each civilization, as it advanced, those who could afford it chose the luxury of a withdrawing-place." **- Phyllis McGinley -**

"We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government." **- William Orville Douglas -**

"Education is the most powerful weapon which you can use to change the world." **– Nelson Mandela –**

"Education is not the answer to the question. Education is the means to the answer to all questions." **- William Allin -**

6.1 Introduction

In this research, the current state of the healthcare sector in South Africa was analysed. Through studying the level of technology adoption in the healthcare sector, it was realised that the healthcare environment is rapidly moving towards technology-based information systems. This led to a realization of the impact this has on the security and privacy of health information.

Healthcare organisations play host to extremely sensitive information. In the modern era, healthcare organisations must ensure that they are able to withstand the onslaught of threats to healthcare information. One particular type of threat agent comes in the form of the organisation's own employees. The damage that can be caused by such employees, whether

intentionally or otherwise, can have a devastating effect on a healthcare organisation, both economically and on the organisation's reputation.

The problem addressed in this research was how organisations in the South African healthcare environment can sensitize, skill and educate their employees about information security in a way that ensures they have the means of protecting security and privacy issues with regard to patient information, and ensures that what they have taught their employees, is applied effectively.

Through an extensive literature study, it was learnt that a SETA programme can be an effective mechanism for an organisation to teach its employees about information security. It was further learnt that in order for a SETA programme to be effective, it must be geared towards the audience that it serves. With cognisance of these facts, the research proposed a role-based security education, training and awareness model to address the problem statement of the research.

6.2 Benefits of the RB-SETA Model

The RB-SETA model offers the following advantages to healthcare organisations:

6.2.1 **Appropriate allocation of resources** to the right elements of a SETA programme

The model ensures that the necessary elements of the SETA learning continuum are addressed in a focused manner when designing a SETA programme. Before designing the SETA programme, the model requires a detailed analysis of security education, training and awareness requirements, for each role identified in the establishment. This ensures that the needs of each role are fulfilled. With the SETA programme being role-based and not a "one size fits all" solution, security areas are

addressed in the order in which they need attention and with the appropriate emphasis.

6.2.2 **Adequate performance** by healthcare personnel in their security-related duties

SETA programmes which ignore the context of the attendees tend not to deliver the results that are envisaged. The approach advocated by the RB-SETA model will be more effective, thereby resulting in personnel satisfying the envisaged requirements of the programme. Therefore, healthcare personnel will be able to perform their security-related tasks adequately.

6.2.3 **Reduced** number of security incidents

When the frame of mind, skill set and knowledge of employees are honed to the level at which it should be, it will inevitably contribute to a decrease in the number of security incidents experienced by the organisation. Organisations lose money when security incidents negatively impact on their daily operations. With less incidents, money will be saved as it will not be used to repair damages or, in the worst case, reputation.

6.2.4 **Increased** trust shown by the public in healthcare organisations

An overall increase in the SETA level of an organisation, will filter through to dampen the public's concerns about security and privacy issues. In the same way, a security incident (e.g. transgression of privacy) will cause panic and distrust. This will be countered if the RB-SETA model is applied by healthcare establishments in the running of their SETA programmes. A member of the public will feel much more positive about going to a healthcare establishment knowing that their personal healthcare

information will be protected and under no circumstances will it be given out without their consent.

6.2.5 Return-on-Investment (ROI)

The application of the RB-SETA model will ensure that the organisation's SETA programme is effective. This, in turn, will contribute to a decrease in the number of security incidents, which will cost the organisation less money. Management will therefore experience a tangible ROI which will help to ensure that resources are again allocated in the next budget to keep developing and running the SETA programme.

It is more difficult to quantify intangible ROIs, but suffice to mention that if the SETA programme stops a privacy infringement from taking place, then the ROI can be quantified as the amount that would have been spent to resolve the transgression.

6.3 Limitations

The limitations of the proposed solution are:

- The effectiveness of the solution is not guaranteed as the implementation will depend entirely upon the healthcare organisation that will be implementing it;

- Due to scope limitations, there was no mechanism in place to measure the effectiveness of the proposed solution;

- The data used to formulate the problem statement and proposed solution was obtained through an extensive literature study. The model is therefore a theoretical solution to the problem, with no real-world practical implementation of the model having been done.

6.4 Chapter Overview

This section aims to provide a summary of the research conducted throughout this study and shows where the objectives of the research as set out in Chapter 1, were met.

6.4.1 Chapter 1 - Introduction

Chapter 1 commenced by motivating why it is important to protect patients' healthcare information through discussing two examples of breaches in privacy. A number of concepts were introduced and briefly discussed, these being the healthcare environment, security and privacy issues in the healthcare sector and general SETA principles. The chapter stated the problem statement, objectives, and the methodology used to meet these particular objectives.

6.4.2 Chapter 2 – The Healthcare Sector and Technology Adoption in South Africa

Sub-Objective

- Investigate the current state of the South African healthcare sector.

Research Questions

- What are the strategic imperatives of the South African National Department of Health and how is the healthcare sector made up in terms of resources and expenditure?
- Has there been an increase in technology adoption in the South African health sector to the extent that it is contributing to the effective interpretation and dissemination of health information?

Chapter 2 provided an in-depth look into the South African healthcare sector. It was ascertained that the South African government is well underway with initiatives to reform this sector. From the governments'

point of view, it was determined why there is a need for better cooperation between the private and the public healthcare sectors. The chapter also looked at how technology can be beneficial for the healthcare sector and how South Africa is doing in terms of adopting technology into the national healthcare system.

The chapter concluded that the South African healthcare sector is well under reform, although much remains to be done in order to truly bring about reform as confessed by the Minister of Health (Department of Health, 2006). One of the factors having an impact on the current state of inequity is expenditure and the way that resources are being allocated to the private and the public healthcare sectors. Lastly, it was realized that with the move towards the electronic environment, there is a need to consider the issue of right to privacy as enshrined in the South African Constitution, as well as the protection of healthcare information in general.

6.4.3 Chapter 3 – Privacy and Security Issues in the Healthcare Sector

Sub-Objective

- Identify the requirements for and legal obligation to the security and privacy of patient healthcare information.

Research Question

- What are the requirements for the security and privacy of patient healthcare information and is there a legal liability?

Chapter 3 started off by discussing the general nature of healthcare information. The chapter then investigated the need to protect the security and privacy of healthcare information. Various examples of incidents concerning breach of security and privacy of healthcare information, were listed. This confirmed the need to have measures in place to protect this information. Over and above these needs, it was also

shown that there is a legal liability towards protecting healthcare information. A brief overview of legal instruments in this regard, with specific focus on the legal acts that South African healthcare organisations have to comply with, was provided.

With consideration for the needs, requirements and legal liability to protect healthcare information, it was concluded that a healthcare organisation must employ mechanisms to inform its employees about information security.

6.4.4 Chapter 4 - General Security Education Training and Awareness Principles

Sub-Objective

- Discuss SETA best practices and generally accepted principles.

Research Question

- Which best practices in security education, training and awareness are relevant in the design, development and implementation of a SETA programme?

Chapter 4 introduced the concept of a SETA programme and that its learning is divided into the three elements of Awareness, Training and Education, which comprise the learning continuum defined by the NIST (NIST 800-50, 2003). Why employees need to be security-aware and how organisations can encourage a culture of security awareness amongst their employees were discussed. It was then emphasised that in order for healthcare personnel to perform their security-related tasks adequately, they have to learn practical skills to an approved level of competency. This is done in the form of conducting security training for employees. It was further discovered that security education is targeted at security professionals and those employees whose jobs require expertise in security. As a result, many organisations do not include security education as part of their SETA programmes.

After discussing the elements of the learning continuum in detail, the process of designing, developing and implementing a SETA programme was considered, including requirements for post-implementation activities. The chapter also reiterated that humans continue to be a security threat within their organisations and that organisations must instil a culture of security awareness amongst its employees in order to reduce the number of security incidents. This set the stage for the proposal of the RB-SETA model in Chapter 5.

6.4.5 Chapter 5 – A Role-Based SETA Model for the South African Healthcare Environment

Sub-Objective:

- Through logical argumentation, propose a role-based SETA model for the South African healthcare environment.

Research Question

- How can education, training and awareness be used to effectively solve the problem of a lack of awareness, skills and knowledge in maintaining the security and privacy of health information?

Chapter 5 was dedicated to constructing the primary output of this research. This chapter proposed a role-based SETA programme which ensures that healthcare professionals know enough, do enough and feel good enough (have a positive mind-set) with regard to information security. The concept behind the model is the use of an ETA Mix that is derived from an ETA profile for a particular role. The ETA profile is brought about by considering the three components of education, training and awareness. The ETA profile is then constituted by documenting the requirements in terms of the acceptable behaviour (training), attitude (awareness) and knowledge (education) about information security for each role. From this, the ETA Mix is determined.

The ETA Mix ensures that the proposed RB-SETA model addresses the requirements towards security education, training and awareness in a combination unique to each role at a healthcare organisation. This ensures a more effective SETA programme for each role.

6.4.6 Chapter 6 – Conclusion

The conclusion of the research is done in this chapter. The benefits of the RB-SETA model and future research directions are also discussed.

6.5 Future Research

A valuable follow-up on the research reported on in this dissertation, will be to apply the proposed solution at a healthcare organisation in South Africa. This can be done using an action research approach to test and improve the model in iterative steps.

Another avenue that can be explored is for the government to develop a generic SETA programme for the South African healthcare environment (public sector), based on the principles of the RB-SETA model. In this scenario the government can take the responsibility for:

- Ensuring that public healthcare establishments implement the SETA programme;
- Monitoring the effectiveness of the SETA programme at the various levels (i.e. nationally, provincially, districts, etc); and
- Setting targets for the healthcare organisations in terms of the ETA levels required of their staff complement.

Whereas the afore-mentioned suggestions for future research hinge on the application of the model in a practical setting, there is also further research required with regard to the model's operation as such. For example, a detailed study is required to further investigate the ETA profile and ETA mix. This could include determining which role players must be

involved as well as a measurement mechanism to determine whether the ETA mix is sufficient, in the post-implementation phase of the SETA programme.

6.6 Conclusion

In this chapter, it was illustrated that all of the objectives that were established at the beginning of this research project, were accomplished. The information covered in various chapters of the dissertation was reviewed and ideas for future research were suggested.

When many socio-economic needs of citizens are trying to be fulfilled, it becomes really difficult to concentrate on problems of one particular sector within the government structure. The case is the same in South Africa. Healthcare is one of the most important socio-economic factors, be it in a developing or a developed country. With socio-economic needs escalating in South Africa, it becomes complicated to ensure that the healthcare sector is well run.

Nevertheless, it remains important to ensure that issues that can impact negatively on the South African healthcare sector are correctly addressed. Of particularly importance are infringement of patients' rights to privacy and breach of the security of health information. So, it becomes necessary for healthcare personnel to handle patient healthcare information appropriately. This can be achieved through running effective SETA programmes.

At the conclusion of this dissertation, it is apt to reflect on Kevin Mitnick's statement quoted at the start of chapter 5, that his success in hacking, depended on the willingness of people to bypass policies and procedures. This calls attention to the importance of security education, training and awareness programmes. It is believed that this research and its outputs have contributed to making SETA programmes more effective, more

focused and of greater benefit to organisations in addressing the “human factor”.

“Vision without action is only a dream.
Action without vision is merely passing the time.
Vision with action will change the world”
– Joel Barker -

References

A Guide to Privacy for Small Business. (n.d.). Retrieved April 9, 2006 from http://svc004.wic001g.server-web.com/publications/bizguide.doc.

ANC. (1994a, May). *A National Health Plan for South Africa*. Retrieved June 1, 2006 from http://www.anc.org.za/ancdocs/policy/health.htm.

ANC. (1994b). *A National Health Plan for South Africa.* Retrieved June 1, 2006 from http://www.anc.org.za/ancdocs/pr/1994/pr0101d.html.

Arkansas' Enterprise Architecture. (n.d.). *Personnel Security*. Personnel Security Guidelines. Retrieved March 23, 2006 from http://www.techarch.state.ar.us/domains/security/resources/personnel_sec_guidelines.doc.

Asia, B., Pillay, Y. (2003). *Districts and Development: National Newsletter, July 2003*. Retrieved March 14, 2006, from ftp://ftp.hst.org.za/pubs/govdocs/dhs/dhs0703.pdf.

Baker, B. (2001). *Security Education for Users: A Starting Place for Network Administrators.* Retrieved September 28, 2006 from http://www.sans.org/reading_room/whitepapers/infosec/600.php.

Beresford, B. (2007, December). *Medical Inequality Grows*. Mail & Guardian, Friday, 7 December 2007, (p.8). Retrieved December 30, 2007 from http://www.hst.org.za/uploads/files/sahr07_mgp8.pdf.

Blecher, M., & Thomas, S. (2004). Health Care Financing. In P. Ijumba, C. Day, & A. Ntuli (Eds.), *South African Health Review 2003/04*. Durban, South Africa: Health Systems Trust.

Bradshaw, D. & Buthelezi, G. (1996). Health Status. In D. Harrison, P. Barron, & J. Edwards (Eds.), *South African Health Review 1996* (pp 19-59). Durban, South Africa: Health Systems Trust.

Buckovich, S.A., Rippen, H.E., & Rozen, M.J. (1999). *Driving Toward Guiding Principles: A Goal for Privacy, Confidentiality, and Security of Health Information*.

CalOHI Office of HIPAA Implementation. (2005). *Background Document: Security Awareness and Training*. Retrieved March 23, 2006 from www.ohi.ca.gov/calohi/docs/PM_2005-57_ Exhibit_7_Awareness_&_Training_Background_Document.doc.

Committee on Standardization of Data and Billing Practices. (2003). *Recommendations of the Committee on Standardization of Data and Billing Practices.* Retrieved April 19, 2006, from http://www.medicalschemes.com/publications/ZipPublications/Presentations%20And%20Reports/StandardisationManual.pdf.

Commonwealth of Pennsylvania. (n.d.). *Managing Unsatisfactory Employee Performance*. Retrieved December 10, 2007 from http://www.cybersecurity.state.pa.us/portal/server.pt/gateway/PTARGS_0_2_10889_1176_254212_43/http%3B/enctcapp099%3B7087/publishedcontent/publish/cop_general_government_operations/oa/oa_portal/hrm/bwpd/wppd/performance_management/managing_unsatisfactory_performance_pamphlet.doc.

Computers at Risk. (1991). Safe Computing in the Information Age. Systems Security Study Committee. *Computer Science and Telecommunications Board Commission on Physical Sciences, Mathematics and Applications, National Research Council*. National Academy Press.

Council for Medical Schemes (2002). *Draft Recommendations of the Committee on Standardization of Data and Billing Practices, Research and Monitoring.*

CSL Bulletin. (1993, October). Retrieved December 13, 2007 from http://www.itl.nist.gov/lab/bulletns/archives/csl93-10.txt.

Day, C., & Gray, A. (2007). Health and Related Indicators. In S. Harrison, R. Bhana, & A. Ntuli (Eds.), *South African Health Review 2007* (pp 215-343). Durban, South Africa: Health Systems Trust.

Definition of a Role. (1949). In Chambers' Etymological English Dictionary (3rd ed., p. 549). London and Edinburgh: Chambers.

Department of Health. (2006). *Strategic Plan 2006/07 - 2008/09*. Retrieved March 14, 2006 from http://www.doh.gov.za/docs/misc/stratplan/2006-2009/index.html.

Du, W., Shang, W., & Xu, H. (2006). A Novel Approach for Computer Security Education using Minix Instructional Operating System. *Computers and Security*, *25*: 190-200. Retrieved September 9, 2006 from http://0-www.sciencedirect.com.echea.ru.ac.za/science?_ob=MImg&_imagekey=B6V8G-4HP6G1X-1-1&_cdi=5870&_user=1378441&_orig=search&_coverDate=05%2F31%2F2006&_sk=999749996&view=c&_alid=457873955&_rdoc=1&wchp=dGLbVzz-zSkzk&md5=f83a4dc0069e4afa3585832c039445b7&ie=/sdarticle.pdf.

Ehealth: The South African Context. (2006). Retrieved December 31, 2007 from http://www.mrc.ac.za/ikmd/nov2006/ehealth.pdf.

Englebardt, S.P, & Nelson, R. (Eds.). (2002). Health *Care Informatics: An Interdisciplinary Approach*. St. Louis, Missouri, USA: Mosby.

Federal Agency Security Practices. (2000). *Information Security and Privacy Training for [the Agency] Information System Security Officers*. Retrieved March 16, 2006 from http://www.iwar.org.uk/comsec/resources/fasp/ISSO-course-slides.ppt.

Feldman, R.S. (1999). *Understanding Psychology.* Fifth edition. McGraw-Hill College. Boston, River Ridge, IL.

Furnell, S.M., Gennatou, M., & Dowland, P.S. (2002). A Prototype Tool for Information Security Awareness and Training. *Logistics Information Management*, *15* (5/6): 352-357. Retrieved may 10, 2006 from http://www.emeraldinsight.com/Insight/ViewContentServlet?Filename=Published/EmeraldFullTextArticle/Articles/0880150503.html.

Garrett, C. (2004, July). *Developing a Security-Awareness Culture – Improving Security*

Decision Making. Retrieved August 21, 2006 from http://www.sans.org/reading_room/whitepapers/awareness/1526.php?portal=b855ab43616647bdb088fe68e1c09483.

Gilbert, C. (2003). *Developing an Integrated Security Training, Awareness, and Education Program*. Retrieved May 10, 2006 from http://www.sans.org/reading_room/whitepapers/awareness/1160.php.

Guenther, M. (2001a). *Security Awareness and the Five Aspects of Security*. Retrieved April 4, 2006 from http://www.iwar.org.uk/comsec/resources/sa-tools/Standard-of-practice-Security-Awareness.pdf.

Guenther, M. (2001b). Security *Awareness Program: Information, Physical and Personal Security.* Retrieved March 15, 2006 from http://www.iwar.org.uk/comsec/resources/sa-tools/Security-Awareness-Program.pdf.

Guenther, M. (2001c). *Security Awareness Quiz Questions*. Retrieved April 4, 2006 from http://www.iwar.org.uk/comsec/resources/sa-tools/Security-Awareness-Quiz-Questions.pdf.

Guenther, M. (2001d). *Security Awareness Workshop Trainer Notes Version 1.0*. Retrieved April 4, 2006 from http://www.iwar.org.uk/comsec/resources/sa-tools/Trainers-Notes-for-Security-Awareness-01.pdf

Guenther, M. (2003). *Security Awareness Benchmarking and Metrics*. Retrieved April 4, 2006 from http://www.iwar.org.uk/comsec/resources/sa-tools/Security-Awareness-Benchmarking-and-Metrics.pdf.

Harrison, S. (2007, December). *Highlights from the SAHR 2007: The Role of the Private Sector within the South African Health System*. Retrieved December 30, 2007 from http://www.hst.org.za/uploads/files/sharrison_sahr07.pdf.

Harrison, S., Bhana, R., & Ntuli, A. (2007). The Role of the Private Sector within the South African Health System. In S. Harrison, R. Bhana, & A. Ntuli (Eds.), *South African Health Review 2007* (pp vii-xvi). Durban, South Africa: Health Systems Trust.

Health Care. (2005). Retrieved October 1, 2007 from http://www.bls.gov/oco/cg/cgs035.htm#related.

Health Technology Assessment. (n.d.). *Discussion Document on a Strategy for the Future*. Retrieved November 22, 2005 from http://www.sahealthinfo.org/hta/htadiscussion.pdf.

Healthcare Design. (2004). *Applying Design and Colour to Healing*. Retrieved December 31, 2007 from http://www.healthcaredesignmagazine.com/ME2/dirmod.asp?sid=&nm=Articles&type=Publishing&mod=Publications%3A%3AArticle&mid=8F3A7027421841978F18BE895F87F791&tier=4&id=CE4D29D5889E4B55A465AA1F2E7EF4E1.

Healthcare Environment: Department of Health (n.d.). Retrieved December 31, 2007 from (04) http://www.dh.gov.uk/en/Policyandguidance/Organisationpolicy/Healthcareenvironment/index.htm.

Hedberg, C. (2003). *2003 South African Health Review*. Retrieved September 2, 2005 from http://www.hst.org.za/uploads/files/Information_Systems.pdf.

Herold, R. (2003). *Information Security and Privacy Awareness Materials Design and Development*. Retrieved April 4, 2006 from http://www.delcreo.com/delcreo/free/docs/Awareness%20Materials%20Design%20and%20Development.pdf.

Hinson, G. (2005). *The Value of Information Security Awareness*. Retrieved August 21, 2006 from http://www.noticebored.com/The_value_of_security_awareness.pdf.

Hodge, J., & Miller, J. (1997). *Information Technology in South Africa: The State-of-the-Art and Implications for national IT Policy*. Retrieved March 15, 2006 from http://www.commerce.uct.ac.za/economics/staff/jhodge/Documents/stprcw~1.pdf.

Horrocks, I. (2001). Security Training: Education for an Emerging Profession? *Computers and Security*, *20*: 219-226. Retrieved September 26, 2006 from (03) http://0-www.sciencedirect.com.wam.seals.ac.za/science?_ob=MImg&_imagekey=B6V8G-43GH3W9-6-1&_cdi=5870&_user=1378441&_orig=search&_coverDate=05%2F01%2F2001&_sk=999799996&view=c&_alid=456278120&_rdoc=6&wchp=dGLbVzz-zSkzV&md5=adf7e9d7c7b0069f12a7119e979208f0&ie=/sdarticle.pdf.

HST (Health Systems Trust). (2007a). *Health Expenditure % of GDP*. Retrieved December 31, 2007 from http://www.hst.org.za/healthstats/79/data.

HST (Health Systems Trust). (2007b). *Health and Management Information Systems (HMIS) Projects*. Retrieved December 31, 2007 from http://www.hst.org.za/generic/91#nhis.

Ijumba, P., & Barron, P. (Eds.). (2005). *South African Health Review 2005*. Durban, South African: Health Systems Trust.

Information Week. (2006). *Government Report Finds Health Care Privacy Breaches Rampant*. Retrieved December 31, 2007 from http://www.informationweek.com/news/showArticle.jhtml?articleID=192501900.

Institute of Health Systems. (n.d.). *Health Informatics*. Retrieved March 16, 2006 from http://www.ihsnet.org.in/HealthInformatics/healthinforma.htm.

International Medical Informatics Association (IMIA). (2000, October). Recommendations of the International Medical Informatics Association (IMIA) on Education in Health and Medical Informatics. *Methods of Information in Medicine*, *39*: 267-277.

Irvine, C.E., Thompson, M.F., & Allen, K. (n.d.). *CyberCIEGE™: An Information Assurance Teaching Tool for Training and Awareness*. Retrieved September 28, 2006 from http://www.cisr.nps.edu/downloads/05paper_cc_ttool.pdf.

Katsikas, S.K. (2000). Health Care Management and Information Systems Security: Awareness, Training or Education? *International Journal of Medical Informatics*, *60*: 129-135. Retrieved September 6, 2007 from http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6T7S-422FH9Y-8-3&_cdi=5066&_user=1378441&_orig=search&_coverDate=11%2F01%2F2000&_sk=999399997&view=c&wchp=dGLzVzz-zSkWb&md5=d0be385649699a15b2e85226104cc501&ie=/sdarticle.pdf.

Kaur, H. (2001). Introduction and Education of Information Security Policies to Employees in My Organisation. Retrieved September 28, 2006 from http://www.sans.org/reading_room/whitepapers/awareness/411.php.

Kruger, H.A. & Kearney, W.D. (2005). Measuring Information Security Awareness: A West Africa Gold Mining Environment Case Study, *In: Proceedings of the 2005 ISSA Conference, Johannesburg, South Africa, ISBN:1-86854-625-X,* 29 June – 1 July 2005.

Kruger, H.A., & Kearney, W.D. (2006). A Prototype for Assessing Information Security Awareness. *Computers and Security, 25*: 289-296. Retrieved September 14, 2006 from

http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6V8G-4JW7WMD-1-2&_cdi=5870&_user=1378441&_orig=search&_coverDate=06%2F30%2F2006&_sk=999749995&view=c&wchp=dGLbVzW-zSkzV&md5=14716e258aefe3487486b035bcf6e108&ie=/sdarticle.pdf.

Labruyere, J-P. (2006, May). *Protecting your Enterprise: The Top 10 Aspects to Consider*. Retrieved December 14, 2007 from http://www.infosecwriters.com/text_resources/pdf/SETA_SHight.pdf.

Lesson 12: Training and Awareness Programs. (2006). Retrieved April 7, 2006 from http://ia.gordon.army.mil/iaso/lesson12.htm.

Mbeki Thabo, President: South Africa. (2005). *Presidency Department Budget Vote*. May 2005.

McIntyre, D., & Thiede, M. (2007). Health Care Financing and Expenditure. In S. Harrison, R. Bhana, & A. Ntuli (Eds.), *South African Health Review 2007* (pp 35-46). Durban, South Africa: Health Systems Trust.

Mechael, P.N. (2002). Integrating Information and Communication Technology to Improve Global Health: A Conceptual Framework. Retrieved March 16, 2006 from http://www.ukglobalhealth.org/content/Text/Integrating_Information_and_Communication_Technology_to_Improve_Global_Health.doc.

Medical College of Georgia. (n.d.). *Privacy and Information Security Awareness Training*. Retrieved March 23, 2006 from http://www.mcg.edu/audits/PrivacyandInformationSecurityAwarenessTraining080405.ppt.

Michener, H.A & Delamater, J.D. (1994). *Social Psychology.* Third edition. Harcourt Brace College Publishers. Orlando, Florida.

Mitnick, K., & William, L. S. (2002). *The Art of Deception.* Indianapolis, United States of America: Wiley Publishing, Inc.

Munley, M. (2004, April). *Moving from Consciousness to Culture: Creating an Environment of Security Awareness*. Retrieved August 21, 2006 from

http://www.sans.org/reading_room/papers/download.php?id=1439&c=1e325150c88f9beecba280f7ec59fcb8.

Murray, F., & Dopson, S. (2002). *Changing Medical Technology: Complexity or Chaos?* (A Discussion Paper), The Nuffield Trust. 2002.

National Department of Health. (2004). *The Closed Health Broadcast Channel*. Retrieved March 14, 2006, from http://www.doh.gov.za/docs/pamplets/chbc.pdf.

National Department of Health. (2005). *Strategic Planning Newsletter No 3, November 2005*. Retrieved April 20, 2006 from http://www.doh.gov.za/docs/newsletter/stratplan/nov05.pdf.

National Department of Health. (2007, April). A Policy on Quality in Health Care in South Africa. Retrieved December 13, 2007 from http://www.doh.gov.za/docs/policy/healthcare-f.html.

NIST. (2001). *Security Awareness*. Retrieved April 4, 2006 from http://www.iwar.org.uk/comsec/resources/fasp/SecurityAwareness.pdf

NIST 800-12. (1995). *An Introduction to Computer Security: The NIST Handbook*. NIST Special Publication 800-12. Retrieved May 10, 2006 from http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

NIST 800-16. (1998). *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. NIST Special Publication 800-16. U.S. Government Printing Office, Washington. Retrieved April 8, 2006 from http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.

NIST 800-50. (2003). *Building an Information Technology Security Awareness and Training Program*. NIST Special Publication 800-50. U.S. Government Printing Office, Washington. Retrieved April 9, 2006 from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

Office of The Federal Privacy Commissioner. (2002, December 21). *A Privacy Checklist for Small Business*. Retrieved April 9, 2006 from http://www.privacy.gov.au/publications/checklist.pdf.

Olzak, T. (2006). Strengthen Security with an Effective Security Awareness Program. Retrieved August 14, 2006 from

http://adventuresinsecurity.com/Papers/Build_a_Security_Awareness_Program.pdf.

Opening Address by the Minister of Health at the Launch of the 2007 South African Health Review (SAHR) Cape Town, 05 December 2007. (2007). Retrieved December 30, 2007 from http://www.hst.org.za/uploads/files/minister_sahr07.pdf.

Patel, A. (2002). IT Security Training in the Healthcare Environment. In E.B. Barber et al. (Eds.), *Security Standards for Healthcare Information Systems.* Amsterdam: IOS Press.

Recruiting - Employee Recruitment: Recruiting Talented Employees. (2007). Retrieved December 10, 2007 from http://humanresources.about.com/od/recruiting/Recruiting_Employee_Recruitment_Recruiting_Talented_Employees.htm.

Richard Bland College Information Technology Services. (2004). *Richard Bland College Information Technology Services Presents: User Security Awareness Training 2004*. Retrieved August 14, 2006 from http://www.rbc.edu/ITS/Security_Awareness_Training_2004.ppt.

Role. (2007). In *Dictionary.com*. Retrieved October 19, 2007 from http://dictionary.reference.com/browse/role.

Schlienger, T. & Teufel, S. (2003). Information Security Culture – From Analysis to Change, *South African Computer Journal, 31*:46-52.

Schultz., E. (2004). Security Training and Awareness – Fitting a Square Peg in a Round Hole. *Computers & Security*, *23*: 1-2. Retrieved September 26, 2006 from http://0-www.sciencedirect.com.echea.ru.ac.za/science?_ob=MImg&_imagekey=B6V8G-4BJ76RM-2-1&_cdi=5870&_user=1378441&_orig=search&_coverDate=02%2F29%2F2004&_sk=999769998&view=c&_alid=456226539&_rdoc=1&wchp=dGLbVzz-zSkzS&md5=4c35807c1f18b6d87e06c79983a22819&ie=/sdarticle.pdf.

Secretary Thompson, Seeking Fastest Possible Results. (2004, May). Retrieved April 22, 2006 from http://www.hhs.gov/news/press/2004pres/20040506.html.

Shaw, V. (2002). "The Development of an Information Systems for District Hospitals", *Proceedings of the 7th IFIP 9.4 Working Conference*, Krishna, S. and Madon, S. (eds.), Bangalore, India.

Siponen, M.T. (2000). *A conceptual foundation for organisational information security awareness*. *Information Management & Computer Security*, *81*: 31-41. Retrieved December 13, 2007 from http://www.emeraldinsight.com/Insight/ViewContentServlet?Filename=/published/emeraldfulltextarticle/pdf/0460080104.pdf.

South African Information Technology Industry Strategy. (2002). *ICT Diffusion and ICT Applications in Usage Sectors Executive Summary*. Retrieved March 14, 2006 from http://www.trigrammic.com/downloads/ICT%20Diffusion%20-%20Executive%20Summary.pdf.

Stenbakk, B-E., & Oie, G.R. (2004). *Role Models in Healthcare*. Retrieved December 28, 2007 from http://www.pvv.ntnu.no/~gunnarre/studies/for/rmhcStenbakkOie.pdf.

Swanson, M., & Guttman, B. (1996). *Generally Accepted Principles and Practices for Securing Information Technology Systems*. Retrieved May 11, 2006 from http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf.

The Privacy and Security Working Group. (2003). *Report and Findings June 5, 2003*. Retrieved March 16, 2006, from http://www.connectingforhealth.org/resources/pswg_report_6.5.03.pdf.

The South African Telemedicine System. (n.d.). Retrieved December 31, 2007 from http://www.kznhealth.gov.za/telemedicine1.pdf.

Thompson Launches "Decade of Health Information Technology". (2004, July). Retrieved April 22, 2006 from http://www.hhs.gov/news/press/2004pres/20040721a.html.

Thompson, M.E. & von Solms, R. (1998). Information Security Awareness: Educating Your Users Effectively, *Information Management & Computer Security, 6*(4):167-173.

Towards Greater Equity in Health Care. (2004, June). Retrieved June 1, 2006 from http://www.doh.gov.za/docs/sp/2004/sp0611a.html.

United States Department of Health and Human Services. (2004). *News Release: Secretary Thompson, Seeking Fastest Possible Results, Names First Health Information Technology Coordinator*. Retrieved April 22, 2006, from http://www.hhs.gov/news/press/2004pres/20040506.html.

University of California San Francisco. (2005). *Security Awareness and Training*. Retrieved March 21, 2006 from http://www.radiology.ucsf.edu/staff/docs/Security_Aware_Training_RAD.pdf.

University of the Witwatersrand. (2004). Aids Law Project: Privacy and Confidentiality. Retrieved May 17, 2006 from http://dedi20a.your-server.co.za/alp/images/upload/20040713_PrivacyCon.pdf.

U.S. Department of Commerce. (2003, April). *Chapter 3 – Security Education and Awareness*. Retrieved April 6, 2006 from http://www.wasc.noaa.gov/wrso/securitymanual/Section%20I%20-%20Chap%203.pdf.

WHO (World Health Organisation). (2007) *Core Health Indicators*. Retrieved December 31, 2007 from http://www.who.int/whosis/database/core/core_select_process.cfm.

Wilson, M., & Hash, J. (n.d.). *Information Technology Security Awareness, Training, Education, and Certification*. Retrieved May 10, 2006 from http://www.itl.nist.gov/lab/bulletns/bltnoct03.htm.

Wright, M.A. (1998). *The Need for Information Security Education*. Retrieved September 28, 2006 from http://0-www.sciencedirect.com.echea.ru.ac.za/science?_ob=MImg&_imagekey=B6VNT-3W2910B-7G-1&_cdi=6187&_user=1378441&_orig=search&_coverDate=08%2F31%2F1998&_sk=980019991&view=c&_alid=457873955&_rdoc=7&wchp=dGLbVzz-zSkzk&md5=9152798f87fa51daf86bda4c68657659&ie=/sdarticle.pdf.

Wright, M.A. (n.d.). *Assessing the Impact of Security Education Initiatives on Critical Infrastructure Protection*. Retrieved September 28, 2006 from http://0-www.sciencedirect.com.echea.ru.ac.za/science?_ob=MImg&_imagekey=B6VNT-43SVCPB-G-1&_cdi=6187&_user=1378441&_orig=search&_coverDate=08%2F01%2F2001&_sk=979989991&view=c&_alid=457873955&_rdoc=4&wchp=dGLbVzz-zSkWb&md5=5cdfcd8043d0a748cf2f11cc5b6a4900&ie=/sdarticle.pdf.

Yngström, L. (1996). Security Training and Education for IT Professionals. *International Journal of Bio-medical Computing*, *43*: 105-113. Retrieved September 26, 2006 from http://0-www.sciencedirect.com.echea.ru.ac.za/science?_ob=MImg&_imagekey=B7GH2-4G05T4X-J-1&_cdi=20166&_user=1378441&_orig=search&_coverDate=10%2F31%2F1996&_sk=999569998&view=c&_alid=456278120&_rdoc=9&wchp=dGLbVlb-zSkWz&md5=6bf846744a932a6ece7e90478b887b24&ie=/sdarticle.pdf.

Appendix A

Paper presented in the Proceedings of the 6th Annual Information Security South Africa Conference, 05-07 July 2006, Sandton, South Africa

A ROLE-BASED SECURITY AWARENESS MODEL FOR SOUTH AFRICAN HOSPITALS

Ophola Maseti[a], Dalenca Pottas[b]

a Department of Information Technology, Nelson Mandela Metropolitan University

b Department of Applied Informatics, Nelson Mandela Metropolitan University

[a] omaseti@nmmu.ac.za, +27 82 6766910, PO Box 77000, Port Elizabeth, 6031

[b] dalenca.pottas@nmmu.ac.za, +27 41 5049100, PO Box 77000, Port Elizabeth, 6031

ABSTRACT

The use of electronic systems to access information is advancing rapidly. Many aspects have to be considered in regards to such high availability of information, for example, training people how to access and protect information, motivating them to use the information extensively, ensuring adequate levels of security, confronting ethical issues and maintaining the availability of information at crucial times. This is especially true in the health sector, where access to critical data is often vital. This data must be accessed by different kinds of people with different levels of access.

However, accessibility often leads to vulnerabilities. The health sector deals with very sensitive data. People's medical records need to be kept confidential; hence, security is very important.

This paper firstly provides an overview of how South Africa is doing compared to the rest of the world as regards to central accessibility of health information as well as the level of technology adoption. A brief investigation of security and privacy-related issues which hinge on the central accessibility of this data is reported on. A model is developed which can be used to create a security awareness checklist. Such a checklist constitutes a self-assessment tool for care-givers in the South African health sector, to gauge awareness in regards of information security and privacy.

KEY WORDS

Health Sector, Health Information Systems, Security and Privacy, Security Awareness

A ROLE-BASED SECURITY AWARENESS MODEL FOR SOUTH AFRICAN HOSPITALS

1 INTRODUCTION

The success of both the public and the private the health care system being dependent on the ability to consolidate information from a variety of sources has been reached as the general consensus in the South African health care environment (Committee on Standardization of Data and Billing Practices, 2003).

The use of electronic systems to access information is advancing rapidly. Many aspects have to be considered in regards to such high availability of information, for example, training people how to access and protect information, motivating them to use the information extensively, ensuring adequate levels of security, confronting ethical issues and maintaining the availability of information at crucial times. This is especially true in the health sector, where access to critical data is often vital. This data must be accessed by different kinds of people with different levels of access.

However, accessibility often leads to vulnerabilities. The health sector deals with very sensitive data. People's medical records need to be kept confidential; hence, security is very important.

It is always necessary for information to be accessible especially in the health sector. Such accessibility (or availability) is further augmented in an integrated environment. For example, a Health Information System (HIS) may be linked to laboratory systems that give the results of certain tests on patients, to emerge with specific data. This data must then be transferred to the patients' medical records automatically without human intervention.

In South Africa, the use of electronic systems in the health sector to share patient information has been slow. The initial plan was to form the National Health Care Management Information System partially by the public and private sector. The formation of this system would ensure proper management of hospitals as well as the key functions and service requirements of the health sector. Thus far, the implementation of this system has not been successful as it is not available in all provinces.

Regardless of the level of integration and / or technology adoption, the fact remains that information of a very sensitive nature, is exposed to human intervention on various levels (e.g. nurses, administrative staff, general practitioners and specialists). In this scenario, it is important for each person to be aware of the requirements in terms of security and privacy, especially from a legal perspective.

This paper firstly provides an overview of how South Africa is doing compared to the rest of the world as regards to central accessibility of health information as well as the level of technology adoption. A brief investigation of security and privacy-related issues which hinge on the central accessibility of this data is reported on. A model is developed which can be used to create a security awareness checklist. Such a checklist constitutes a self-assessment tool for care-givers in the South African health sector, to gauge awareness in regards of information security and privacy.

2 THE HEALTH SECTOR: TRANSFORMATION AND TECHNOLOGY ADOPTION

2.1 Reform of the South African Health Sector

South Africa has had an unfortunate event of the apartheid in the past. Back then, there were too m any policies from the apartheid government that were not allowing all South Africans access to proper health care. Now that South Africa is a free and democratic country, all the damage from the past would need to be unravelled by the government. All legislation, organisations and institutions related to health had to be reviewed with the involvement of the complete transformation of the national health care delivery system (ANC, 1994a).

"When we started the term of office of this government in 2004 we set ourselves a series of goals which we sought to achieve when this term ends in 2009. These goals are contained in a document which we called "Strategic Priorities for the Health Sector 2004-2009 (popularly called the 10 Point Plan)"" (Department of Health, 2006, Online). It clearly shows that the government is aware that the health sector needs to have serious changes to be effective, towards the benefit of all South Africans. The Department, as is reflected in the Plan will improve the health facilities and the quality of care that is provided in these facilities, both clinics and hospitals. In this regard they plan to introduce a hospital improvement plan in April 2006. With respect to health programmes, two programmes have been prioritised in line with the decisions taken by World Health Organization, Regional Office for Africa (WHO/AFRO). During 2006 a TB Crisis Plan will be launched to deal more decisively with the burden of disease from TB as well as an Accelerated HIV Prevention Plan (Department of Health, 2006, Online). The government must have some means to measure their achievements against their goals.

In order to know your progress in terms of achieving your goals, it is imperative that you reflect on what you were able to achieve thus far. "These priorities are based on an assessment of what we have achieved in the past 10 years and what work remains to truly transform the health system to better meet the needs of all those who live in South Africa. Whilst we are justifiably proud of our achievements we need, in the next five years to work hard with our partners to strengthen the health system so that we can provide accessible, good quality health services to all" (Department of Health, 2004, Online). The government is willing to compromise and work very hard with its partners and bring fresh ideas that would ensure that the health system of South Africa is strengthened. This is good news for the South African public, as the government has had problems with ensuring that delivery in the Department of Health is of good quality.

The District Health Information System, despite persistent problems with data quality, data flows and utilisation of data/information has been a major achievement and largely a unifying force across the country (Hedberg, 2003, Online). The Department of Health further adopted a National Policy on Quality in 2001 (Department of Health, 2004, Online). Based on the national policy, all the provinces have now established provincial policies and quality assurance units to lead and co-ordinate efforts on quality improvement, there are also complaints systems and procedures in place for all the provinces and the national department. To support this notion even more, the government has to ensure that there is proper infrastructure and

resources throughout the whole country. This can be done by investing and spending money wisely in the health sector.

Calle Hedberg (2003), who is a Researcher and a Systems Designer at the Health Information Systems Programme claims that the Government expenditure on Health Care Information Systems has not changed in line with the shift towards the Primary Health Care approach (Hedberg, 2003, Online). The author alleges that 90 to 95% is spent on advanced Hospital Information Systems in larger hospitals, which is believed to be why the South African health sector has a slow improvement in technology. The South African government has been spending a small amount of money in making sure that good health care is affordable for all South Africans. South Africa spends R550 per person per year on health care which is only 5% of GDP (ANC, 1994b, online). The World Bank estimates that ten times more should be spend to provide basic health care for all. To date, around 2004, this GDP value has gone up to 8.5% (Department of Health, n.d., Online). In order to ensure that South Africa does really reach its true potential with regards to the reformation of the health sector, there must be proper planning and corruption should be prevented by all means.

It must be derived from the fact that the state is the largest social institution, therefore its capital, human resources, managerial, technological and organisational requirements must be expected to reflect the society from which it originates (Mbeki, 2005). The Government is surely paying attention with regards to the reformation of the health sector in South Africa. The Government has got a good plan from a strategic level but the implementation of the strategy at the lowest level has not been successful because of certain factors. Amongst these factors, shortage of staff members and inappropriate infrastructure can be included but not limited to them.

Usually organisations have excellent strategies, but the mistake that they make is not communicating these strategies to the people that generate the value of the organisations (National Department of Health, 2005, Online). The document released by the National Department of Health in 2005 says that if this can be applied to the Department of Health it will mean that the front line workers and managers should be engaged in the development of these plans and the strategy of the Department of Health should be communicated to those that will assist to achieve the strategy; however, these things to be effortless in theory but they seem to be rocket science in practice. With the strategies involving technology and the health care sector involving a lot of people referred to as general practitioners, there must be a way to distinguish that whenever there is a new strategy the front line workers are included as part of that strategy.

It seems as if the Health Care Information Systems and Monitoring and evaluation is viewed as mainly a technology acquisition process aimed at purchasing a turn-key universal solution, this can cost billions of rands in the end (Hedberg, 2003, Online); it should be rather viewed as a long-term socio-cultural, political, and technical development process with short-term practical and functional applications that work. People are the ones that really make technology work. As people form part of the organisational culture, it should not be forgotten how they are going to be catered for as well as how they would be addressed whenever there is a new technology being introduced within the organisation.

2.2 Technology Adoption in South Africa

Health information technology yields huge savings as it has the potential to greatly improve health care (United States Department of Health and Human Services, 2004, Online). Since the future of health care delivery institutions lies in cost-effective health care, health care delivery institutions will need and use information technology to meet their client demands and stay competitive (Institute of Health Systems, n.d., Online). Furthermore, the author states that general purpose information technology solutions are usually insufficient for special needs of the health sector.

The South African government is under a process of enhancing the South African health sector by involving the Constitution of South Africa and the Bill of Rights. This process has to involve information technology within it. There has to be a way that this process can be measured to see if there is any progress in terms of utilising technology. Member states of the World Health Organisation (WHO) should have established "structures and processes to ensure continued improvement of the quality of health services and an appropriate development and utilization of technology", the obligation of establishing effective procedures for the evaluation of the advantages and relevance of Health Technology both in developmental as well as routine use is also tied to this (Health Technology Assessment, n.d., Online). This subject is addressed on Goal 31 of the World Health Organisation's "Health For All" strategy. So it is evident that the focus on the regulation and management of Health Technology is not a South African trend alone.

Both the European Union (EU) and globally (G-8) have brought forward within them health care as one of the sectors in society with great potential for Information and Communication Technology (ICT) and with great benefits to be gained through their application in the Information Society (South African Information Technology Industry Strategy Project, 2002, Online). The South African Information Technology Industry Strategy Project (2002) further states that governments must be encouraged and in particular health ministries to facilitate the implementation of what is commonly called "e-health", international surveys reveal a huge number of public sector and industry-based studies to raise awareness of the potential of Information and Communication Technology. With the implementation of "e-health" being emphasised at most developing countries all over the world, South Africa have hastened the concept of a District Health Information System

The District Health Information System has been implemented in all the provinces of South Africa; however the use of this data effectively has been minimal. An assessment of many hospitals in the Eastern Cape in 1999 indicated that: "Data is collected 'at all levels in hospitals, but most of it is never used'. Indicators are submitted to the district offices, but give a 'very bland picture of administrative activities, and no feeling of what goes on inside hospitals'. 'Registers are non-standardized, and tend to be anarchic, and hand written', and often on an assortment of different types of paper and books. 'Analysis of data is minimal at all levels'." (Shaw, 2002). If the implementation of the District Health Information is to be successful, the data collected must be analysed thoroughly and be used extensively whenever there is a need to do so. There seems to be a lack of integration between the hospitals and the district management, which is costing the advancement of the government in trying to improve the services offered by the health sector, (Hedberg, 2003, Online) professes that there have been persistent problems with data quality, but data flows and utilisation of data/information, has been a major achievement and

largely a unifying force across the country. District managers must work together with the hospital managers maybe by having meetings quarterly to discuss the data that has been generated for the past three months and taking decisions thereafter that are going to benefit the public that is making use of the health services. By doing so, they would be ensuring that the utilisation of the health care data is enhanced.

In terms of data capture and use, most health districts in the country are still at level 1 (data is being captured but its quality and use requires major improvement), level 3 (data of good quality collected and used for service improvements) is the target for all health districts (Asia & Pillay, 2003, Online). The authors further say that to reach this target in all health districts, it is important that provincial, local government and district information officers work with clinic supervisors and clinic managers.

To further improve the level of health awareness by making use of technology amongst all South Africans, the Department of Health decided to develop a South African National Telemedicine System so that it could be able to offer health care services to the most distant South African rural areas. Patients who usually visit the clinics would be able to learn from the content provided by the Telemedicine System. The objective of developing this system was to narrow the gap between the poorly resourced rural areas and the urban areas. This technology promised to provide a way of sharing skills and cutting through problems caused by geographic isolation, poor transport and infrastructure as well as scarcity of skilled health professionals; this led to a Memorandum of Understanding being signed between Sentech (national signal carrier for both radio and television in South Africa) and the Department of Health in 1999 for the establishment of a Health Channel using satellite technology (National Department of Health, 2004, Online). This Telemedicine System initiative has helped to improve the level of health awareness in South Africa amongst the patients and the health care workers.

Like any employee that works for an organisation, if that employee is slotted to a role within that particular organisation, they get used to that role and become good at it. It is essential for the health care institutions to ensure that the health care professionals are able to utilise all the new technologies that the institution brings forth. A major determinant of the rate of adoption of information technology in the health care sector is the personal computing skill of health care professionals (Institute of Health Systems, n.d., Online); furthermore, if doctors, nurses and other health care professionals are comfortable with personal computing, the rate of information technology adoption in health care institutions is likely to be faster.

2.3 Technology Adoption Internationally

An explosion of health information systems with associated benefits to health and human prosperity is being witnessed, with the liberalisation of health care and telecommunications policies spreading across every continent (McDonald, n.d., Online). The author further states that “high technology” has less importance than another gigantic problem that is facing lesser developed countries, hunger.

It is alleged that in member countries of the Organisation for Economic Co-operation and Development, spending on health care is already outpacing economic growth. An understanding of larger context within which governments manage health care systems, and administrators make decisions concerning the services that will be provided must be the first thing to arise whenever any discussion about the adoption

of innovations by health care systems takes place (Canadian Biotechnology Advisory Committee, 2004, Online). In America, the Institute of Medicine estimates that between 44 000 and 98 000 die each year because of lack of medical records (The White House, 2004, Online). “By computerizing health records, we can avoid dangerous medical mistakes, reduce costs, and improve care.” (Bush, 2004).

In Canada, the Commission of the Future of Health Care paid considerable attention to the issue of medical necessity and did not directly address the impact that biotechnology will have on the health care system (Commission on the Future of Health Care in Canada, 2002). The commission concluded that “the definition of what is considered medically necessary and covered under the [*Canada Health*] *Act* needs to be updated to reflect the realities of our contemporary health care system”.

3 PRIVACY AND SECURITY ISSUES IN THE HEALTH SECTOR

Some of the long-standing needs and concerns in our society have been privacy, confidentiality, and security of personal health information especially to health care providers and the public (Buckovich, Rippen & Rozen, 1999). Health care providers and organisations is the legitimate need to access information to deliver quality health care, which is also important to the public. Since information technology has been proven beyond doubt as a way of living nowadays, the health sector has had no choice but to integrate information technology into most of its systems. With this shift came the urgent need to balance privacy and access and to develop guiding principles, policies, and legislation to ensure that the most valuable information to the public is protected safely from any unauthorised authorities. With the use of information technology on the rise, access to sensitive and personal information has been easy for more individuals and entities.

As the electronic medical record offers the promise of improved care and increased efficiency, introducing information technology into the health care creates new risks to privacy as well as new means to protect privacy (The Privacy and Security Working Group, 2003, Online). There are potential risks associated with automation and sharing of patients medical records and patients are well of these risks. Patients can be lead to withholding information that could be vital to their care, from their clinicians based on these concerns. In return, the value of the patients’ medical records can be reduced to other clinicians treating the patient and to researchers and public health officials. This can be caused by the exclusion of sensitive information by the clinician as a result of the concerns about privacy and security.

One of the most important things for organisations in the modern era is to train its employees on the value that the organisation places on privacy of its customers’ information, as well as how to implement the privacy protection of health information.

Audit trails can be implemented by large institutions with electronic health records. These audit trails can track both accesses and changes to records without degrading system performance. Audit systems can be a good tool to deter employees from accessing information they are not authorised, as they are aware that they actions are being captured by the system. Audit trails can be very effective if any incidents are reported, then investigated if someone breached against the rules.

4 A ROLE-BASED AWARENESS MODEL FOR SOUTH AFRICAN HOSPITALS

4.1 General SETA Principles

The purpose of computer security awareness, training, and education is to enhance security by: improving awareness of the need to protect system resources; developing skills and knowledge so computer users can perform their jobs more securely; and building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems (National Institute of Standards and Technology, 2004, Online). When the SETA program is to be carried out, it must be known who is going to be educated about this program and what should they be taught.

NIST 800-16 (1998), in the NIST model states that the learning of the security education program is a continuum. It starts with awareness, constructs to training and then develops into education.

The three levels of the learning continuum can be portrayed as follows:

Awareness: As the learner is only the recipient of information and does not actively participate (NIST 800-16, 1998), the purpose of an awareness program is to stimulate and motivate those being trained to care about security and to remind them of important security practices (National Institute of Standards and Technology, 2004, Online). Posters and flyers are very helpful in assisting with this level of the learning continuum.

Training: Training focuses on providing the knowledge, skills, and abilities specific to an individual's role and responsibilities relative to IT systems (Federal Agency Security Practices, 2000, Online). There are usually two groups of users that are targeted for training, the general users and the advanced users or users with specialised skills.

Education: The Education level of the learning continuum integrates all of the security skills and competencies of the various functional specialities into a common body of knowledge. Most organisations opt not to include security education as part of their awareness and training programs as it is part of employee career development.

Each person has a responsibility to every other person. All IT services are at risk when an incident happens. It is of importance that all the role players in an organisation be educated about the vitality of security. We therefore propose a role-based security awareness model to be implemented for South African hospitals.

4.2 A Role Based Awareness Model

The proposed model is depicted in Figure 1.

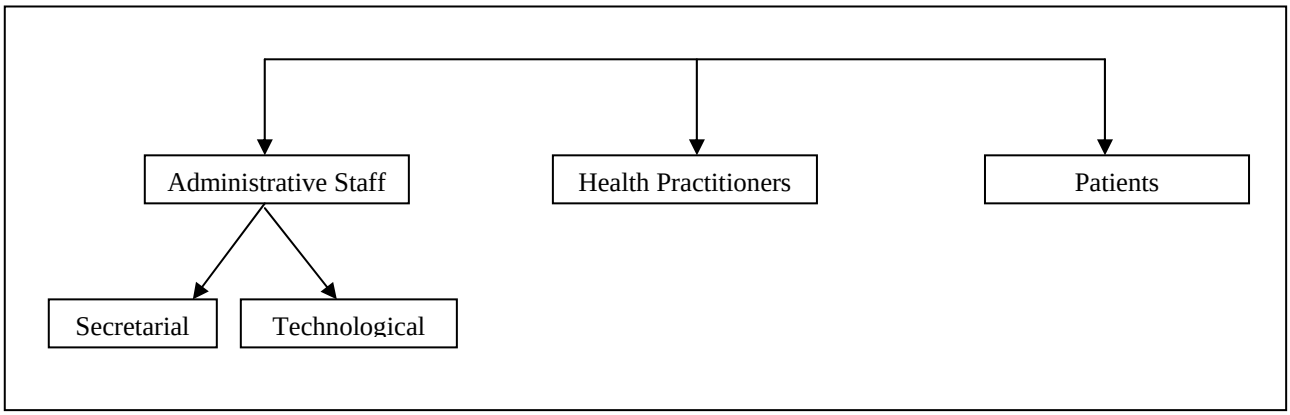


Figure1. A Role-Based Security Awareness Model

The model that is proposed will address role-based awareness as its title implies. In our study we are taking a look at a hospital, be it private or public. The hospital usually consists of health practitioners and administrative staff.

Health Practitioners: These are the people that look after the patients, day in and day out. They diagnose, talk about confidential issues with the patients and handle the sensitive records of the patients. It is imperative that they are aware of privacy issues that relate to the patients.

Administrative Staff: These are divided into two sections, the secretarial and the technological staff. The secretarial staff deal more with patients checking in and checking out. They can also check patient records for specific doctors, but only to a specific level. They are the weakest link. The Technological Staff are more concerned about computer security and information security. They do not deal directly with the patients, but more with patient data that is stored on the hospital's computer systems.

Awareness as an element from SETA that is intended to allow individuals to recognise IT security concerns and respond accordingly. As the learner is the recipient of information in awareness activities, it is increasingly important that the programme targets the audience that it is intended for. This will maximize the benefits achieved from such a programme. It is pointless running a programme for all staff, where most of the information is too generic or too specific to be applicable.

If an organisation's awareness program is properly designed, developed and implemented; it is only left to the employees to make certain that technology is being used properly. In order for technology to work, it needs people.

4.3 Sample Questionnaires

From the literature survey that we have carried out, we have deducted that there is a need to have a security awareness checklist in the health sector. This checklist will be distributed to several role-players at hospitals that fall under the private or the public sector. It will be limited to administrative staff and health practitioners. It will be addressing issues that pertain to the patients' privacy whilst they are within the boundaries of the hospital as well as what happens during the time that leads them to being there and when they have left. These issues will be viewed from the patient's

perspective, the health practitioner's perspective as well as the administrative staff's perspective.

Accordingly, some questions are listed which could form a part of the awareness checklists.

4.3.1 Administrative Staff: Technological

1. Are all departmental staff aware of security processes?

2. Did the staff receive computer security awareness training?

3. Are staff members aware of the Privacy Policy and their responsibilities?

4.3.2 Administrative Staff: Secretarial

1. Do you regularly have education sessions that focus on aspects of privacy, confidentiality or security to promote best practice in your area?

2. Do staff members know where the privacy website is located on the Intranet?

3. Are medical records left unattended in your work area?

4.3.3 Health Practitioner: Doctor

1. Do you use fair and lawful ways to collect personal information?

2. Do you have a short document that sets out clearly expressed policies on the way you manage personal information and make it available to anyone who asks for it?

3. If a patient asks, what sort of personal information you hold about them, what purposes you hold it for and how you collect, use and disclose that information. Do you take reasonable steps to let them know?

4.3.4 Health Practitioner: Hospital Manager

1. What measures will be taken to ensure the personal information is secure during transit and storage?

2. Will the personal information be used for any secondary purposes?

3. Have all the staff members in the medical practice been reminded of good personal health information management? It may be appropriate for all family practice staff to sign confidentiality agreements related to their use of personal health information.

4.3.5 Patient

1. When your personal health information was collected, did the Health Practitioner ensure that you are aware of the reasons as to why they are collecting your personal information?

2. Are you able to access your own personal health information in an appropriate way?

3. Are you allowed to correct this information using a process that tracks any amendments?

5 CONCLUSION

This paper took a look at the reformation of the South African health sector that has been initiated by the South African Government. We compared these developments with what is already available out there internationally. It was realised that the South

African health sector needs a checklist to ensure that all the role-players are sufficiently aware of issues pertaining to the security and privacy of health information. Hence we proposed a role based security awareness model. This model ensures that all role players in the health sector are targeted according to their level and method of exposure to and utilization of health information. With the level of privacy awareness being very low in the South African health sector, designing a role-based SETA program by making use of the proposed role based awareness model would ensure that this problem is addressed aptly.

6 REFERENCES

ANC. (1994a). *A National Health Plan for South Africa*, African National Congress, Johannesburg, South Africa.

ANC. (1994b). *A National Health Plan for South Africa.* Retrieved June 1, 2006 from http://www.anc.org.za/ancdocs/pr/1994/pr0101d.html.

Asia, B., Pillay, Y. (2003). *Districts and Development: National Newsletter, July 2003*. Retrieved March 14, 2006, from ftp://ftp.hst.org.za/pubs/govdocs/dhs/dhs0703.pdf.

Buckovich, S.A., Rippen, H.E., & Rozen, M.J. (1999). *Driving Toward Guiding Principles: A Goal for Privacy, Confidentiality, and Security of Health Information*.

Bush, G. W., President: United States of America. (2004). *State of the Union Address, January, 20, 2004*. Retrieved April 23, 2006, from http://www.whitehouse.gov/infocus/technology/economic_policy200404/chap3.html.

Canadian Biotechnology Advisory Committee. (2004). *Biotechnology and the Health of the Canadians*. Retrieved March 16, 2006, from http://cbac-cccb.ca/epic/internet/incbac-cccb.nsf/vwapj/BHI-Final_Dec-13-04-E.pdf/$FILE/BHI-Final_Dec-13-04-E.pdf.

Committee on Standardization of Data and Billing Practices. (2003). *Recommendations of the Committee on Standardization of Data and Billing Practices.* Retrieved April 19, 2006, from http://www.medicalschemes.com/publications/ZipPublications/Presentations%20And%20Reports/StandardisationManual.pdf.

Department of Health. (2004). *Strategic Priorities for the National Health System, 2004-2009.* Retrieved November 22, 2005 from http://www.doh.gov.za/docs/policy/stratpriorities.pdf.

Department of Health. (2006). *Strategic Plan 2006/07 - 2008/09*. Retrieved March 14, 2006, from http://www.doh.gov.za/docs/misc/stratplan/2006-2009/foreword.pdf .

Department of Health. (n.d.). *Health Sector Strategic Framework 1999-2004: Socio-Economic and Health Status.* Retrieved June 9, 2006 from http://www.doh.gov.za/docs/policy/framewrk/chap02.html.

Federal Agency Security Practices. (2000). *Information Security and Privacy Training for [the Agency] Information System Security Officers*. Retrieved March 16, 2006 from http://www.iwar.org.uk/comsec/resources/fasp/ISSO-course-slides.ppt.

Health Technology Assessment. (n.d.). *Discussion Document on a Strategy for the Future*. Retrieved November 22, 2005, from http://www.sahealthinfo.org/hta/htadiscussion.pdf.

Hedberg Calle. (2003). *2003 South African Health Review. Health Information Systems Progress with Caveats – an Integration Perspective*. Retrieved September 2, 2005 from http://www.hst.org.za/uploads/files/Information_Systems.pdf.

Herold, Rebecca. (2003). *Information Security and Privacy Awareness Materials Design and Development*. Retrieved April 4, 2006, from URL:htttp://www.delcreo.com/delcreo/free/docs/Awareness%20Materials%20Design%20and%20Development.pdf.

Institute of Health Systems. (n.d.). *Health Informatics*. Retrieved March 16, 2006, from http://www.ihsnet.org.in/HealthInformatics/healthinforma.htm.

Mbeki Thabo, President: South Africa. (2005). *Presidency Department Budget Vote*. May 2005.

McDonald, M.D. (n.d.). *Health Information Infrastructure in Developing Countries*. Retrieved March 16, 2006, from http://www.greenstar.org/GHI/Developing%20Countries.htm

MediaPro. (n.d.). *Privacy Direction 101: Awareness*. Retrieved April 4, 2006, from http://www.mediapro.com/products/corpComp/pdf/PD101%20Product%20Sheet.pdf.

National Department of Health. (2004). *The Closed Health Broadcast Channel*. Retrieved March 14, 2006, from http://www.doh.gov.za/docs/pamplets/chbc.pdf.

National Department of Health. (2005). *Strategic Planning Newsletter No 3, November 2005*. Retrieved April 20, 2006 from http://www.doh.gov.za/docs/newsletter/stratplan/nov05.pdf.

Shaw, V. (2002). "The Development of an Information Systems for District Hospitals", *Proceedings of the 7th IFIP 9.4 Working Conference*, Krishna, S. and Madon, S. (eds.), Bangalore, India.

South African Information Technology Industry Strategy Project. (2002). *ICT Diffusion and ICT Applications in Usage Sectors Executive Summary*. Retrieved March 14, 2006, from http://www.trigrammic.com/downloads/ICT%20Diffusion%20-%20Executive%20Summary.pdf.

The Privacy and Security Working Group. (2003). *Report and Findings June 5, 2003*. Retrieved March 16, 2006, from http://www.connectingforhealth.org/resources/pswg_report_6.5.03.pdf.

The White House. (2004). *Transforming Health Care: The President's Health Information Technology Plan*. Retrieved April 23, 2006, from http://www.whitehouse.gov/infocus/technology/economic_policy200404/chap3.html.

United States Department of Health and Human Services. (2004). *News Release: Secretary Thompson, Seeking Fastest Possible Results, Names First Health Information Technology Coordinator*. Retrieved April 22, 2006, from http://www.hhs.gov/news/press/2004pres/20040506.html.