A FRAMEWORK FOR THE SECURE USE OF PORTABLE STORAGE DEVICES:
A SOUTH AFRICAN HIGHER EDUCATION PERSPECTIVE

by

Jonathan S. Rothman

Treatise

submitted in partial fulfilment of the requirements for the degree of

MAGISTER TECHNOLOGIAE: BUSINESS INFORMATION SYSTEMS

in the

FACULTY OF ENGINEERING, THE BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

at

Nelson Mandela Metropolitan University

Supervisor: Prof. D. Pottas

February 2009
Dedication

My sincerest thanks and appreciation are extended to:

- **God, Almighty** for making a way possible where there was none.
- My Supervisor, **Professor Dalenca Pottas**, for the professional manner in which she assisted me as well as the continual giving of her own precious time, dedication and encouragement which led to the finishing of the paper.
- **Steve Viljoen** for his contribution in helping getting the project rolling.
- My Family and Friends for their support, in particular my friend **Shereen Dupreez** who encouraged me to finish.
- To **Debbie** for all the time she spent proofreading and her assistance with finding material to work with.
DECLARATION BY CANDIDATE

NAME: JONATHAN SEAN ROTHMAN

STUDENT NUMBER: 9742046

QUALIFICATION: MAGISTER TECHNOLOGIAE: BUSINESS INFORMATION SYSTEMS

TITLE OF PROJECT: A FRAMEWORK FOR THE SECURE USE OF PORTABLE STORAGE DEVICES: A SOUTH AFRICAN HIGHER EDUCATION PURSPECTIVE

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: 23 FEBRUARY 2009
# Table of Contents

Tables and Figures ........................................................................................................ iv  
Abstract ......................................................................................................................... v  

1. Chapter 1: Introduction and Background ................................................................. 01  
1.1 The South African Higher Education Landscape ................................................... 02  
1.2 Universal Serial Bus Connectors and Devices ....................................................... 04  
1.3 Risks Created ......................................................................................................... 06  
1.4 Problem Statement ............................................................................................... 08  
1.5 Limitations in Scope ............................................................................................. 09  
1.6 Research Objectives ............................................................................................ 09  
1.7 Research Methods ............................................................................................... 10  
1.8 Layout of Treatise ............................................................................................... 10  
1.9 Conclusion ......................................................................................................... 12  

2. Chapter 2: The South African Higher Education Landscape ................................ 14  
2.1 Introduction ........................................................................................................... 15  
2.2 SA Education – Governance Structures .............................................................. 16  
2.3 The Merger of SA Higher Education Institutions ................. ............... 18  
2.4 The Use of Technology in Higher Education ...................................................... 22  
2.5 Conclusion ......................................................................................................... 29
4.5.2 Access control ........................................................................................ 64
4.5.3 Intrusion detection .................................................................................. 64
4.5.4 Firewall ................................................................................................... 64
4.5.5 Public key infrastructure ....................................................................... 64
4.5.6 Malicious code protection ....................................................................... 65
4.5.7 Vulnerability scanners ............................................................................ 65
4.5.8 Forensics ................................................................................................ 65
4.5.9 Media sanitizing ...................................................................................... 65
4.6 Conclusion ......................................................................................................... 67

5. Chapter 5: Conclusion ...................................................................................... 68

5.1 Introduction ........................................................................................................ 69
5.2 Chapter Overview ............................................................................................... 71
  5.2.1 Chapter 1 – Introduction ............................................................................ 71
  5.2.2 Chapter 2 – The South African Higher Education Landscape ................. 72
  5.2.3 Chapter 3 – Portable Storage Devices .................................................... 73
  5.2.4 Chapter 4 – A Framework for the secure use of Portable Storage .......... 74
      Devices at South African Higher Education Institutions
  5.2.5 Chapter 5 – Conclusion ........................................................................... 75
5.3 Benefits and Limitations of the Research ........................................................... 75
5.4 Future Research ................................................................................................. 76
5.5 Conclusion ......................................................................................................... 76
References ................................................................................................................ 78
Tables and Figures

Figure 1.1: Layout of Treatise ................................................................. 11
Table 2.1: Mergers of Higher Education Institutions in South Africa ............. 20
Figure 4.1: A Triangular Framework for secure use of Portable Storage Devices..... 47
Figure 4.2: Example – Layer: “By Order”, Category: Laws .................................. 51
Figure 4.3: Example – Layer: “By Order”, Category: Standards ........................ 55
Figure 4.4: Example – Layer: “By Order”, Category: Policies ............................. 57
Figure 4.5: Example – Layer: “By Behaviour”, Category: Awareness ................. 59
Figure 4.6: Example – Layer: “By Behaviour”, Category: Education .................... 60
Figure 4.7: Example – Layer: “By Behaviour”, Category: Training ..................... 62
Figure 4.8: Example – Layer: “By Technology” ............................................. 66
Abstract

South African Higher Education has gone through various changes and challenges, one of these being the merger process. Various Universities and Technikons were forced to merge in an effort to aid the transformation and restructuring of the Higher Education landscape in the post-apartheid era. From an ICT point of view, the merged Institutions ended up with massive and distributed computing facilities. These facilities must be managed and secured and it can be appreciated that the complexity and magnitude of this task is compounded by the large and varied user population (i.e. students) using the facilities.

With the exploding use of mobile consumer devices (such as cell phones, personal digital assistants, MP3 players, portable storage devices such as flash drives, etc), Higher Education Institutions are faced with the even more complex task of managing and securing the computing infrastructure, while large numbers of students can enter computer labs and use these devices at random.

In some circles, portable devices are touted to be the next panacea in higher education. This, together with the popularity these devices enjoy under the student body, makes it a fait accompli that mobile consumer devices are “here to stay”. Therefore, banning these devices from campus computer labs, is not viable. Universities have to find ways to address security issues through the implementation of appropriate protective measures.

This research focuses on finding a solution to mitigating the risks imposed on Higher Education Institutions in South Africa caused by the use of portable storage devices. The research proposes a framework which serves as an outline for the countermeasures that Universities must implement to mitigate the risks inherent to the use of portable storage devices. The scope of the research is limited to flash drives, smart phones and MP3 players.
CHAPTER 1

INTRODUCTION AND BACKGROUND

“The proliferation of consumer devices such as iPods, USB devices, Smart Phones and more, has dramatically increased the risk of intentional and unintentional data leaks and other malicious activity. While most companies have anti-virus software, firewalls, email and web content security to protect against external threats, few realize how easy it is for an employee to simply walk in and copy large amounts of sensitive data onto an iPod or USB stick.”

GFI EndPointSecurity
1.1 The South African Higher Education Landscape

The online Oxford dictionary defines education as orderly instruction, schooling or training given to the young in preparation for the work of life (Oxford University Press, 1989). Higher education, according to the South African Higher Education Amendment Bill, means all learning programmes which lead to one or several qualifications (Higher Education Amendment Bill, 2008). This qualification must be higher than grade 12 or its equivalent in terms of the National Qualifications Framework as reflected in the South African Qualifications Authority Act 58 of 1995 (SAQA, 1995). It includes tertiary education, as reflected in Schedule 4 of the Constitution, that meets the requirements of the Higher Education Qualifications Framework (Staatskoerant, 2008).

The higher education system of a country is important in terms of its human resource requirements and contributes to its development. Higher education has a distinctive and important role to play in the learning society. In particular, higher education must create independent learners. It should enable individuals to grow intellectually, to achieve personal fulfilment, and to contribute fully and at the highest levels to society, the workplace and the nation (International Development Research Centre, 1999).

The emergence of South Africa (SA) into a new democratic order means it has been faced with several challenges in various sectors of the country. One of these sectors is the Higher Education (HE) sector which was affected by various changes. Continuous change and decreasing predictability of the future are some of the primary challenges which affected this sector. Higher education institutions were confronted with unexpected and far-reaching demands. One of the main changes was the transformation and restructuring of the higher education landscape in South Africa through various mergers between HE institutions (Bosch, 2005).

The mergers led to massive and distributed infrastructure at HE institutions which use complicated Information and Communication Technologies (ICTs) (Mahabir, 2008).
ICTs is an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning (SearchCIO-Midmarket, 2004). A review of the education landscape reveals that there has been an increasing interest in technology in many higher education institutions in South Africa since 2000. A larger percentage of university budgets are being spent on ICT infrastructure than in previous years (Czerniewicz, Ravjee, & Mlitwa, 2006).

The SA Government has been putting more funding into Information and Communication Technologies with the understanding that the country needs development in those areas. Over the past two years the SA Government made available additional funds to the traditional Universities to increase the number of trained engineers. Other efficiency and restructuring funds were made available to Universities of Technology to participate in a drive for more technology-savvy graduates (Staatskoerant, 2008).

The term ‘techno-savvy’ is used to describe the technology skill levels of students and indicates a belief by system administrators that current students have an elevated level of ability when seeking and using information found on the Internet and from electronic resources (Combes, 2006). Therefore it can be deduced that the SA Government is funding higher education institutions to establish infrastructure and facilities which enable students to hone their skills in working with electronic resources. In fact, it is not uncommon to see students walking around on campus with an IPod listening to music, to have a phone with an USB connection or to own a flash memory stick to use in the computer lab for transferring data of various types. The increase in technology-savvy students is therefore leading to an increased use of USB devices in higher education institutions.
1.2 Universal Serial Bus Connectors and Devices

Most computers are fitted with one or more Universal Serial Bus (USB) connectors. The term USB stands for Universal Serial Bus, which is an industry-standard specification for attaching computer peripherals. It provides high performance and the ability to plug in and unplug devices while a computer is running. USB was developed by the personal computing and telecommunications industries, including such companies as Compaq, DEC, IBM, Intel, Microsoft, NEC, and NorTel (Northern Telecom) (Apple Computer, Inc., 1999).

USB connectors allow for the attachment of many devices quickly and easily. The computer operating system supports USB, therefore, the installation of device drivers is quick and easy as compared to other ways (parallel ports, serial ports and specially installed cards) of connecting peripherals, which in the past, was slow and tedious. This makes the use of USB devices simple and user-friendly. The USB provides a single, standardized, easy-to-use way to connect up to 127 devices to a computer - nearly all peripherals currently manufactured, contain a USB version (Brain, 2008).

A list of sample USB devices that are available includes:

- Printers;
- Scanners;
- Mice;
- Joysticks;
- Flight yokes;
- Digital cameras;
- Webcams;
- Scientific data acquisition devices;
- Modems;
- Speakers;
• Telephones;
• Video phones;
• Storage devices such as flash drives;
• Network connections; and
• Music devices.

This research focuses on portable devices that have mass storage capacity, are connected via USB and are used by students or staff to move information between computers for various reasons. A mass-storage device is an electronic hardware device that is able to store large volumes of information. It adheres to a protocol for sending and retrieving information over a hardware interface (Axelson, 2006). In the higher education environment, it is conceivable that students will use a USB device to store large volumes of data, such as homework assignments, multimedia PowerPoint presentations, music or video and that they would want to be able to transfer this data to a computer at University.

Previously, storage devices had a limited capacity. In the Sixties, the 8'' floppy disk stored 100 kilobytes, or about 60 typewritten, double-spaced pages of text. The Seventies saw the 5'' disk which held 360K, and in the Eighties, 3'' diskettes emerged, which stored 1.44 megabytes (MB) of data. Nowadays portable storage devices have large capacities and can copy data at high speeds. For example, it is difficult to buy a USB flash drive with a storage capacity below 128MB and some of these devices can copy data at rates greater than 20MB per second (Branzburg, 2004). The technology is both user-friendly and powerful and it seems unimaginable that a person would manage without it. In the past floppy disks were used but were unable to store the amount of data that is now needed. The capacity of a CD-RW might be sufficient but the procedure of burning a disc is not comparable to the ease of plugging a flash drive into the USB port (Hamid, 2006). But this ease of use brings with it increasing risks.
1.3 Risks Created

A risk is the prospect of an acknowledged threat source that exploits a potential vulnerability, the result of which would cause a negative impact to the organization. In higher education institutions, all portable storage devices that can connect to the institution’s computer infrastructure constitute threat sources that can cause harm. Devices such as USB memory sticks, smart phones and IPods can be connected via the USB port of the computer allowing the transfer of data. This transfer could be an automatic synchronization or merely copying data through a “manual” request. The fact is that there is little or no control over the connection.

Memory sticks or flash drives are small devices and can be carried around on a key ring. However, they have the capacity of storing large amounts of different types of information. Data can be uploaded or downloaded to and from the stick, by simply plugging it into the USB port of a computer, laptop or PDA. The speed and size of data transfer makes these devices easy to use and mass data can be transferred quickly.

Security threats inherent to the use of flash drives include (Steele & Wargo, 2007):

- No differentiation between authorized and “rogue” devices;
- No audit or logging of data on devices;
- No centralized control;
- Leakage of sensitive data; and
- Infection from outside data brought into the network on these devices.

This is equally true for mobile phones and IPods. What may seem like an innocent action could result in infection from viruses, or allow for illegal material or unlicensed software to be transferred to the corporate network (Groves, 2004). The IPod is a mobile music player and it was designed for that purpose; but they can be used to copy personal or financial data, intellectual property and other sensitive information
from corporate PCs, often without a trace. The use of an IPod to steal corporate data has gained so much attention lately that it has earned its own name - slurping (Garretson, 2007).

Kelly (2007) in the British magazine, *Computing*, writes that over 80 per cent of mobile media contains unprotected data. Regardless of this statistic, just over half of companies in Britain have taken no steps to secure data held on these devices as revealed by a UK government-backed security survey (Ward, 2006). Wong (2008) in “Risk associated with USB memory sticks and high capacity storage devices”, explains how popular USB storage media is, how easily the device connects and the growing risks it is causing to companies and their clients due to its misuse. The biggest risk posed to companies, according to Wong (2008), was the theft of data by disgruntled employees or the loss of confidentiality as a result of lost, stolen and misplaced USB storage devices.

An article from the BBC News website, written by Ward (2006), states that a survey found that only 33% of firms tell their staff not to use such devices but these firms hardly make any changes on PCs and laptops to stop people from moving data around with USB sticks. Only 10% of those companies interviewed for the survey made an effort to encrypt the confidential data stored on these portable devices.

According to Barnes (2003) USB flash drives and cards that are used in cameras and other mobile devices, can carry PIM (Personal Information Management) data, for example address book, calendar, to-dos and notes data. All this data can be exploited for social engineering, identity theft and other harmful crimes. Social engineering is a collection of techniques used to manipulate people into performing actions or revealing confidential information (Wikipedia, 2008). A survey was conducted by the organizers of InfoSecurity Europe 2003 to gauge how security-conscious workers were about their company information stored on computers. A series of questions was asked, one of them being “what is your password?” to which 75% of the personnel gave the
information away without question and through social engineering, another 15% gave passwords away (Leyden, 2003). The 1995 arrest and conviction of Kevin Mitnick for social engineering and hacking remains one of the most celebrated and controversial cases of its kind, lending support to the popular opinion that hackers are among the most dangerous non-violent “white collar” criminals in society (Steele & Wargo, 2007).

Unlike private corporate networks, which, by their nature, are designed to be “walled gardens” of information, campus networks – due to the need to facilitate collaboration and provide access to information – generally are designed to be more open, and therefore more vulnerable to misuse (Salomon, Cassat, & Thibeau, 2003). Considered together with the increasing use of portable storage devices on university campuses, this underscores the importance of securing the environment.

1.4 Problem Statement

The main problem to be investigated in this research, is that the growing use of portable USB devices at South African Higher Education Institutions is increasing the risk of possible harm to the computing facilities of these institutions. In order to address this problem, the following research questions must be investigated:

• How has the higher education sector changed in South Africa and how have Institutions of Higher Learning adapted to incorporate technology in their environments and teaching practices?
• How have portable storage devices developed in recent years and which risks are posed through the use of these devices in higher education institutions?
• How can the increasing risk of possible harm to the computing facilities through the use of portable storage devices, be countered?
• Can the countermeasures to ensure secure use of portable storage devices in South African higher education institutions, be conceptualized in a framework to serve as a guideline for these institutions?
1.5 Limitations in Scope

As stated in Section 1.2, this research focuses on portable devices that have mass storage capacity, are connected via USB and are used by students or staff to move information between computers for various reasons. It should be noted that due to scope limitations this does not include all portable USB devices, but is limited to:

- USB flash drives;
- Smart phones; and
- MP3 players.

1.6 Research Objectives

The primary objective of this research project is to create a framework for the secure use of portable storage devices in South African Higher Education Institutions. In order to achieve this objective, the following sub-objectives must be addressed:

- Investigate recent changes in the South African higher education landscape and the use of technology at Institutions of Higher Learning;
- Determine the origin and evolution of portable storage devices and consider how their use in higher education institutions is increasing the risk of harm to computing facilities;
- Examine the countermeasures that are available to mitigate the risk of using portable storage devices in higher education institutions; and
- Create a framework for the secure use of portable storage devices in South African higher education institutions, which incorporate the required countermeasures.

In order to achieve these objectives, the following research methods were applied.
1.7 Research Methods

The primary data collection method used in this research is secondary data collection or literature review. A literature study was conducted to review published works about the topics relevant to this research. These include:

- The South African Higher Education Landscape;
- The use of technology in higher education;
- USB flash drives, smart phones and MP3 players;
- Risks created through the use of the afore-mentioned devices; and
- Possible controls to counter these risks.

The sources used to do the literature review were selected based on availability and trustworthiness.

Based on the material gathered, the author used logical argumentation to propose a framework for the secure use of portable storage devices at South African Higher Education Institutions. Brief scenario sketches or examples were provided to explain the components of the framework.

1.8 Layout of Treatise

The layout of the treatise is illustrated diagrammatically in Figure 1.1 and discussed thereafter.
Chapter 1: Introduction
This chapter provides an introduction to the broader areas of concern to be investigated as part of this project, with a view to introducing the problem statement and research objectives. It further provides an overview of the research methods and the chapters to be included in the dissertation.
Chapter 2: The South African Higher Education Landscape
This chapter investigates higher education institutions in South Africa in more detail and their use of technology for educational purposes.

Chapter 3: Portable Storage Devices
This chapter explores the technical workings of (selected) portable storage devices and the resulting risks introduced in the computing facilities at higher education institutions.

Chapter 4: A Framework for the Secure use of Portable Storage Devices at South African Higher Education Institutions
This chapter investigates the countermeasures required to ensure that the use of portable storage devices in the computing facilities of higher education institutions is managed and controlled to minimize the risks involved. The result of this investigation is presented and discussed in the form of a framework.

Chapter 5: Conclusion
This chapter concludes the research by analysing the benefits and limitations of the research and proposing areas for future research. It is shown that the objectives of the research were reached.

1.9 Conclusion

Heydenrych, Higgs and Niekerk (2003) quote a number of authors as warning higher education providers to adapt to provide learners or future workers with new skills as required for an age of regionalism, globalisation and continuing change. Not surprisingly “technology skills” is included on the list of new skills enumerated by these authors. In this Chapter, it was shown that the SA government has increased funding to higher education institutions, exactly for this purpose – to support growth in “technology skills”. It was further shown that SA HEIs have experienced major
changes over the last few years which affected the demographics of university campuses and subsequently campus computing infrastructure. These factors, together with the fact that students have become more technology-savvy and are using a number of portable devices to bring electronic data into campus and conversely, take data off campus, have created vulnerabilities and threats that need to be managed in order to secure the computing infrastructure.

In Chapter 2, the higher education system in South Africa is investigated in more detail to provide information about how this sector is governed and constituted and how technology is used to augment teaching practices.
CHAPTER 2

THE SOUTH AFRICAN HIGHER EDUCATION LANDSCAPE

“In the future, technology will have an increasingly critical impact on the way educational institutions present their services. In South Africa, the challenge in higher education is to redress past inequalities and to restructure the educational system to rise to the challenges of a modern country that can be competitive in the 21st Century.”

Technology and Society Magazine


2.1 Introduction

Every person in South Africa has the right to education. According to the Bill of Rights, contained in the 1996 South African Constitution everyone has the right to a basic education and this includes adult basic education and further education, which the State, through reasonable measures, must progressively make both available and accessible (Burger D., 2008).

This chapter provides background to the South African Higher Education system and its structure. The chapter goes on to explain how various changes in the educational system have affected the landscape. The chapter also shows how technology has played a role in South African Education.

With regard to primary and secondary level education, the Department of Education published the following details in 2006 (Department Of Education, 2006):

- South Africa is made up of 12.3-million learners, some 386 600 teachers and 26 292 schools, including 1 098 registered independent or private schools;
- There are roughly 6 000 high schools (grade 7 to grade 12) and the rest are primary schools (grade 0 to grade 6);
- The average ratio of scholars who are known as "learners" in terms of the South African outcomes-based education system to teachers or educators is 32.6 to one in government-funded public schools, while private schools generally have one teacher for every 17.5 scholars.

At tertiary level, there are more than a million students enrolled in the country’s state-funded Institutions (Isaacs, 2007). South Africa had 36 public higher education institutions (HEIs) in 1994, but this number was reduced to 21 as part of the on-going transformation of the higher education sector through mergers of some institutions. The institutions now comprise 11 universities, 6 Technikons (or Universities of
Technology) and 4 comprehensive institutions (offering both University and Technikon-type programmes) (Teng-Zeng, 2005).

2.2 SA Education – Governance Structures

The Department of Education has seven branches (Burger D., 2008):

- Administration;
- Auxiliary and Associated Services;
- System Planning and Monitoring;
- Quality Promotion and Development;
- GET (General Education and Training);
- FET (Further Education and Training); and
- HE (Higher Education).

A brief overview of the function of each of these branches is provided.

**Administration** - To ensure sound financial and administrative management and internal control for the Department of Education in terms of the Public Finance Management Act, the Public Service Act and other applicable legislation (Department of Education, 2008).

**Auxiliary and Associated Services** provide services including human resources management, vehicle transport and support to provincial education departments on personnel provisioning (National Treasury, 2008).

**System Planning and Monitoring** - Deals with physical planning for schools, financial planning, economic analysis, research coordination and education information managements systems (Monitoring South African Parliamentary Committee, 2006).
Quality Promotion and Development - Provides strategic direction for the development of policies and education programmes to ensure continuous improvement in the quality of teaching and learning (Burger, 2005).

GET - The General Education and Training (GET) branch provides leadership by managing and evaluating programmes for school education, learners with special needs, education management and governance programmes, district development and human resources (HR) in education (Burger D. , 2008)

FET – The Further Education and Training (FET) branch consists of all learning and training from the National Qualifications Framework (NQF) Levels 2 to 4, or the equivalent of Grades 10 to 12 in the school system and National Technical Certificate 1 to 3 in FET colleges (South Africa Online, 2008).

HE – The Higher Education branch is governed by a number of statutory bodies, including SAQA (South African Qualifications Authority) and the CHE (Council on Higher Education) and applicable legislation, for example, the Higher Education Act. These are discussed below.

The South African Qualifications Authority comprises 29 members who are appointed by the Ministers of Education and Labor. The members are identified as national stakeholders in the education and employment sectors. The role of SAQA is to help higher education in terms of registering standards and qualifications in terms of the SAQA Act, 1995 (SAQA, 1995). SAQA accredits all higher education degrees and qualifications based on the guidelines and criteria laid out in the National Qualifications Framework (Sedgwick, 2004).

The Higher Education Act (No. 101 of 1997) sets out the roles and responsibilities of the CHE and its permanent subcommittee, the Higher Education Quality Committee (HEQC), with regard to policy and quality-assurance related matters in the higher
education sector (Higher Education Quality Committee, 2003). The Council on Higher Education (CHE) is assigned the responsibility for producing and setting the standards for all higher education qualifications and for ensuring that they meet SAQA criteria. The CHE was appointed in June 1998 and provides knowledgeable, planned advice on higher education issues to the Minister of Education (Higher Education Act, 1997). CHE is accountable for upholding quality assurance within higher education and training, including program accreditation, institutional audits, program evaluation, and quality promotion (Sedgwick, 2004). The Higher Education Qualifications Framework (HEQF) determines the qualification types, characteristics and purposes of qualifications in terms of South Africa (DOE, SAQA & CHE, 2008).

2.3 The Merger of SA Higher Education Institutions

Various changes and challenges have been observed in various sectors of the country with the emergence of a new democratic order in South Africa. Higher education is one sector which has been inundated with various changes, including mergers, de-racialisation, a new funding framework, and more recently, enrolment capping (Mahabir, 2008).

A merger in higher education is the combining of two or more separate institutions into a single new organizational entity. Its control rests with a single governing body and a single chief executive body and all the assets, liabilities, and responsibilities of the former institutions are transferred to the single new institution (Hall, 2004).

Other changes in South Africa, namely the transition from apartheid to a post-apartheid society have created the conditions for these fundamental changes to all levels of education, including higher education (Jansen, Mergers in South African Higher Education, 2003).
Some of the changes were needed because of the following (Jansen, Jonathan, 2008):

- A system divided by racial inequalities with the white and black institutions bearing the material, cultural and social markings of their separate histories.

- The historically black universities and technikons were - with a few exceptions - deeply entangled in the ongoing conflict, instability and crisis. Students were in conflict with the institutional leadership over their inability to pay tuition and registration fees; staff were in conflict with vice-chancellors; senates confronted councils; councils themselves were deeply divided, especially on the issue of management.

- South African institutions witnessed a dramatic and unexpected decline in student enrolments, a trend that had severe consequences for the struggling black universities. In 1999, for example, the total headcount of enrolments at universities and technikons dropped by 41,000 students (or 7 per cent).

The planned merger of institutions, as suggested by then Minister of Education, Kader Asmal, caused mixed feelings (Hayward, 2002). However, the mergers went ahead and the government began its National Plan for Higher Education which was its blueprint for transforming the 36 existing institutions, with divergent missions that were based on racial grounds, into 21 institutions with new institutional and organisational forms reflected in mission convergence and the creation of a new institutional type, termed the comprehensive institution (Humphrey, 2008).

The new Higher Education landscape comprises three types of institutions: the traditional research-focused university, the university of technology and the new comprehensive university that combines academic and vocationally oriented education and are aimed at enhancing student access and expanding research opportunities and market responsiveness (StudySa, 2008).
The following table (Table 2.1: Mergers of Higher Education Institutions in South Africa) shows a summary of the merged universities and technikons in South Africa.

<table>
<thead>
<tr>
<th>Merged Institution</th>
<th>Originating Institutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>North West University</td>
<td>Merger between the Potchefstroom University of Christian Higher Education, University of the North West and Sebokeng campus of Vista University (1 January 2004)</td>
</tr>
<tr>
<td>University of KwaZulu-Natal</td>
<td>Merger between University of Natal and University of Durban Westville (1 January 2004)</td>
</tr>
<tr>
<td>University of Pretoria</td>
<td>Merger between University of Pretoria, and Mamelodi campus of Vista University</td>
</tr>
<tr>
<td>University of the Free State</td>
<td>Merger between University of the Orange Free State, Qwa Qwa Campus of the University of the North and Bloemfontein campus of Vista University</td>
</tr>
<tr>
<td>University of Johannesburg</td>
<td>Merger between Rand Afrikaans University, East Rand and Soweto campus of Vista University and Technikon Witwatersrand (1 January 2005)</td>
</tr>
<tr>
<td>University of the Western Cape</td>
<td>Merger between Dental Faculty of University of Stellenbosch and the University of the Western Cape</td>
</tr>
<tr>
<td>University of Fort Hare</td>
<td>Merger between University of Fort Hare and East London campus of Rhodes University</td>
</tr>
<tr>
<td>Nelson Mandela Metropolitan University</td>
<td>Merger between University of Port Elizabeth and Port Elizabeth Technikon (including the Port Elizabeth campus of Vista University) (1 January 2005)</td>
</tr>
<tr>
<td>University of Limpopo</td>
<td>Merger between the Medical University of South Africa and University of the North (1 January 2005)</td>
</tr>
<tr>
<td>University of South Africa</td>
<td>Merger between UNISA, Technikon SA and Vudec</td>
</tr>
<tr>
<td>Tshwane University of Technology</td>
<td>Merger between Pretoria Technikon, Technikon Northern Gauteng and North West Technikon (1 January 2004)</td>
</tr>
<tr>
<td>Cape Peninsula University of Technology</td>
<td>Merger between Cape Technikon and Peninsula Technikon (1 January 2005)</td>
</tr>
</tbody>
</table>
Table 2.1: Mergers of Higher Education Institutions in South Africa

The negative effects of mergers can be summarized as follows (Stumpf, 2008):

- The Merger Unit of the Department of Education was insufficiently experienced in the operational issues facing merging institutions. They should have been headed by an ex-Vice Chancellor;
- The absence of a best practice guide, for many of the issues facing merging institutions, caused unnecessary problems;
- The merging institutions suffered from a lack of merger funding during the merger period;
- The merging institutions found it hard to merge and carry on 'as usual' without an increased staff capacity;
- Most merging institutions suffered from student enrolment decreases due to ‘market confusion’ which resulted in funding cuts.

A further negative effect attributed to the mergers is the “bad” state of financial affairs that merged institutions seem to have reached. It is generally agreed upon that the following factors have contributed towards the problem (Hay, Mabokeng, Mapesela, & Driekie, 2006):
• The fragmented further and higher education systems inherited from the previous dispensation;
• The profound inequities and distortions of the above-mentioned systems;
• Incoherent and poor articulation between the various types of further and higher education institutions;
• Declining state subsidy mainly as a result of poor economic growth;
• The impact of new legislation such as the Labour Relations Act resulted in the permanent appointment of temporary workers, increased salaries and the expansion of basic fringe benefits to all members of staff;
• The production and dissemination of knowledge not only by traditional further and higher education institutions, but also by new types of institutions using different modes of delivery; and
• Increased competition in the system from particularly international and private further and higher education institutions.

Interestingly, Lund (2008) reports that the African National Congress (ANC) is planning a review of higher education institutions formed as a result of the mergers, noting that some mergers could be reversed, others could be in for management and operational overhauls and new institutions could also be planned to meet demand. In the mean time, however, the mergers have gone ahead and merger outcomes are judged critically and with few positives in regard of equity effects, efficiency effects, curriculum effects, organisational effects, student effects, staffing effects and physical effects (Jansen, 2003). It appears that the mergers will remain a discussion point on higher education agendas for the foreseeable future.

2.4 The Use of Technology in Higher Education

As stated in Chapter 1 and confirmed by Czerniewicz et. al. (2007), South African Higher Education Institutions continue to increase spending on ICTs. In addition to the
definition of ICTs provided in Chapter 1, Section 1.1, the following definition from Websters (2008) is provided:

*Information and Communication Technology - (ICT) is the study of the technology used to handle information and aid communication. The phrase was coined by Tevenson in his 1997 report to the UK government and promoted by the new National Curriculum documents for the UK in 2000.*

Information and Communication Technology has shaped a new world. These technologies, when correctly harnessed, enable greater access to information, stimulate economic development, enhance opportunities and enable governments to deliver services efficiently to citizens (PNC, 2008). It was noted in a recent Western Cape study of access and the use of ICTs in Higher Educational Institutes in the Western Cape, that when computers were first used, the focus was on administration and infrastructure (Lippert, 1993). It was only from the mid nineties that ICTs shifted into the domain of teaching and learning. It is only since the start of the 21st century that some institutions have started to mainstream ICT into teaching and learning practices across the institution (Brown, 2008).

It has been suggested that ICTs can and do play a number of roles in education. These include the following:

- Providing a means for rethinking teaching practice (Flecknoe, 2002; McCormick & Scrimshaw, 2001);
- Developing the kind of graduates and citizens required in an information society (Department of Education, 2001);
- Improving educational outcomes, for example improving pass rates and enhancing and improving the quality of teaching and learning (Wagner, 2001; Garrison & Anderson, 2003; Jaffer, 2007).
In South Africa, the potential of ICT for both economic and educational motives is well acknowledged; however, limited infrastructure, technological capacity, funding and sustainability of resources, and human resources and expertise hinder its progress (McNeal, 2007). South African universities are considered to be under-equipped even though a relevant education requires “technology skills” to be part of it as shown in Chapter 1, Section 1.9. This was re-emphasised in the National Research and Technology Audit of 1998 (National Research Foundation, 2004). A relevant education is more important than ever, because the current networked world demands a workforce that understands how to use technology as a tool to increase productivity and creativity (Hawkins, 2008).

The government has a strong obligation to ICT in education. South Africa has embraced E-education to improve on the realization of nationwide educational goals. E-education is, according to the University of Pretoria (2008), the design, development and delivery of technology-enhanced, learning experiences which use a variety of media, for example, web-based (online), interactive television broadcasting, video, multimedia CD-ROMs and video conferencing. E-education is about connecting learners to other learners and teachers to professional support services which provide the platforms for learning. Every South African learner, according to the South African Department of Education, must be ICT capable (Facweb, 2008).

The use of information and communication technologies to support learning in South African universities is increasing and Stephen Marquard of the University of Cape Town states that they are "not very far behind the curve" of developed countries in e-learning (MacGregor, 2008). MacGregor (2008) further states that ICT activities are limited by low internet bandwidth and uneven access by students to computers, but that there is widespread experimentation within the constrained African context and that interest is keen.
South Africa is generally well positioned in terms of ICT infrastructure compared to its African counterparts; however, there are a number of key issues in this regard that impact on higher education, including (Brown, 2008; Burger, 2008):

- The number of Internet users is higher than the availability of personal computers which indicates how critical community facilities and work environments are in providing access to ICT;
- Internet costs constitute an important issue for academics and students alike and it is quite fair to say that South Africa is the most expensive country in Africa and one of the most expensive in the world;
- The current limitations in bandwidth impact on the teaching and learning environment and governs what is possible and what is easy to do; and
- It is important to remain conscious of the divides amongst students as access levels remain disparate between the demographic groups.

Computer laboratories can have a life-changing impact on students. They provide core job skills and pre-vocational training in IT for the disadvantaged and at-risk youth populations (Room to Read, 2008). The use of Information Technology (IT) is making possible new student-centered environments where students are guided to acquire the available information they can search for by themselves in different sources (Sayed, 2008).

The providers of information increasingly utilise web and other IT platforms to deliver their resources, therefore, students require IT skills to access the literature in their field. Furthermore, to complete their assignments - from essay writing, to presentations and the analysis of data - students will need to develop skills in accessing and using the appropriate software that is available to support these activities (University of Bermingham, 2008).
One of the most common problems of using ICT in education is to base choices on technological possibilities rather than educational needs (Jaffer, 2007). Oelofse believes that by implementing the right technology (i.e. based on educational needs), it will not only allow for more effective training solutions, but will create a streamlined approach to learning (Oelofse, 2008).

Higher education institutions face strong competition from virtual (or distance) universities. Distance learning is less expensive to support and is not constrained by geographic considerations, therefore, it offers opportunities in situations where traditional education has difficulty operating. Students with scheduling or distance problems can benefit, as can employees, because distance education can be more flexible in terms of time and can be delivered virtually anywhere (CIO-Midmarket, 2008).

Distance learning separates the learner from the educator and it requires that interventions are in place to counter the constraints that this distance poses to the learners and educators. Student assessment is an important challenge for tertiary distance institutions and these institutions therefore use Computer Aided Assessment (CAA) as a tool to assist in this regard. CAA is described as “any instance in which some aspect of computer technology is deployed as part of the assessment process” (Atkinson & Davies, 2000; Tshibalo, 2005).

Distance education provides a unique opportunity for those who wish to study but cannot attend residential institutions because of personal circumstances or occupational obligations (Bruce, Education Online: Learning Anywhere, Any Time, 1999). Virtual universities are described as universities without walls that use the Internet and satellites to deliver their courses and allow teaching resources, libraries, and even laboratories to be shared by people and organizations in widely scattered places (Cappe, 1998).
The University of South Africa (UNISA) is the largest E-education type university in South Africa. It pioneered tertiary distance education in 1946 and continues to do so by using the Internet. There are approximately 130,000 registered Unisa students worldwide (Bruce, 2000). The training of students and staff is conducted by the Electronic Learning Centre of the UNISA library, which is a training venue equipped with thirty computers which were funded by a donation from the Goldfields Foundation in 1997. These were upgraded in 2006; following a second donation from the same corporation (Brown, 2007).

Many examples of interventions in higher education in Africa involve distance and online education. Distance education extends the reach of education to those who are unable to attend a traditional university and it was seen as a solution to help under-resourced universities (Chetty, Buckhalter, Best, Rebecca, Grinter, & Mark, 2007).

The African Virtual University (AVU), another distance education initiative, was first started as a standalone virtual university by the World Bank and it offers courses and degrees online (Chetty, 2007).

Suggestions to improve e-learning include (Unwin, 2008):

- Availability of hardware (particularly computers);
- Faster Internet connectivity/improved bandwidth;
- Improved software;
- Appropriate policies favoring e-learning;
- Provision of technical support for e-learning at a range of scales;
- Lower prices for connectivity;
- Availability of reliable electricity;
- Appropriate content in appropriate languages;
- Awareness raising about the value of e-learning; and
- Improved training for teachers in e-learning at all levels.
Institutions of higher education, whether they employ a direct contact or distance education approach, still face the pressures and challenges of integrating technology into their teaching.
2.5 Conclusion

According to a report of the Council on Higher Education (Martin, Ashley, & Thierry, 2004), change and transformation are currently major forces that are driving South African higher education towards the emergence of a new education landscape. In this chapter the driving forces behind transformation in the SA Higher Education Sector were explained. It was shown that although the mergers, a direct result of transformational motives, went ahead, there is much negativity surrounding it.

The last part of the chapter investigated the role of ICTs at Institutions of Higher Learning. In particular, it is clear that the lack of computing infrastructure has a real and definite impact on the successfulness of e-learning in South Africa.

In Chapter 3, the focus of the discussion shifts to portable storage devices and the impact of their use on university campuses. Specifically the threats posed by the use of these devices are investigated.
The latest major issue facing organizations is the use, either legitimate or otherwise, of USB devices .... There appears to be a rapidly growing level of paranoia as people begin to appreciate what these devices are capable of and how difficult it is to prevent/control their use.

John Jessop, Cryptic Software
3.1. Introduction

Portable storage devices, in particular, have gained in capacity and become ubiquitous in the enterprise environment. However, these devices are usually lacking in security, control and management tools and, in most cases, their use is not covered by a corporate security policy which foresees activities such as audit, backup, encryption or asset management. In most organizations, the use of USB memory sticks, media players and other portable storage devices is out of control. A recent study revealed that two thirds of Information Technology professionals who use removable media at work admit that they do not protect them with encryption (Watson, 2006).

In Chapter 1 it was mentioned that this research focuses on portable devices that have mass storage capacity, are connected via USB and are used by students or staff to move information between computers for various reasons. It was further noted that due to scope limitations this does not include all portable USB devices, but is limited to USB flash drives, smart phones and MP3 players. In this Chapter the investigation of portable storage devices is therefore limited to the mentioned devices, with the intention of investigating their origin and development and the risks that are inherent in using these devices via plugging into the USB port of a computer.

3.2 What Is USB?

In Chapter 1, the term Universal Serial Bus (USB) was explicated. To reiterate, it is a system for attaching peripherals to personal computers using standard physical connections and communication systems. USB allows for “hotplugging” devices (that is adding and removing devices without having to switch the power off) and will also supply power to low consumption devices, negating the need for another power supply (Coates, 2008).
USB flash drives, smart phones and MP3 players are examples of portable devices that can be connected to a computer via USB. The history and technical layout of each of these devices are subsequently discussed in Sections 3.2 – 3.5.

3.3 USB Flash Drives

The first flash drive was manufactured and distributed in Europe under the "disgo" brand name. It was available in four sizes at the time; 8MB, 16MB, 32MB, and 64MB (Rpe4usb.com, 2008). From 2008, USB flash drives are available in 64GB capacity, for example, the world's largest independent manufacturer of memory products, Kingston Technology Company, launched its 64GB USB flash drive in 2008 (My Digital Life, 2008).

Literature reveals that there is no agreement as to who the original creator of the flash drive is with several companies claiming this honor for themselves. The situation is probably complicated by the fact that there are various processes and technologies, which together enabled the creation of flash drives, but which did not develop at the same time. (whatis.com, 2008). In the following discussion some of the manufacturers are mentioned explaining what aspects in the creation of the USB flash drive each company was involved in. Some of these companies ended in rivalry and even court cases to claim the patency for themselves.

USB interfaced NAND memory was invented by Dov Moran and he claims that the first flash drive using this technology was manufactured in 1996 by M-Systems Flash Disk Pioneers, of which he was the founder, Chairman and CEO at the time (Crunchbase, 2008). Toshiba is also recognized as a pioneer in flash technology and is seen as a principal innovator of NAND- and NOR-type flash technology in the Eighties (Irvine, Calif, & Tokio, 2006). Trek was the first company to sell a USB flash drive (called a Thumb Drive) in early 2000 (Enterprise Today, 2008). However, their patent does not
describe the USB flash drive but rather describes a broad family of storage devices which could include the USB flash drive.

In July 2002, Netac obtained a China patent for the invention in a patent titled “Flash Memory Methods and Devices for Digital Processing Systems” (Lerar, 2006). In November 2005, Trek won a patent suit against memory device manufacturers M-Systems Flash Disk Pioneers, FE Global Electronics, Electec and Ritronics Components (Singapore) in Singapore (Kiat, 2008). The list of patents and inventors continues and, therefore, there are many names for the device, for example USB Flash Disk (UFD), Thumb Drive, Pen Drive, Memory Key, Micro Vault, Pocket Drive, Key Chain and Pico Drive (Lightbody, 2007). The term “flash drive” seems to be the most universally accepted name.

USB flash drives actually do not contain a drive, but the term was initially used because UFDs were seen as a replacement for the floppy disk drive to transfer data between personal computers (Hogan, 2007). Floppy drives have limitations because storage needs have increased with an equal demand for higher-performance, removable storage solutions. USB flash drives have gained a lot of momentum and have replaced floppy disk drives as the standard removable storage solution in personal computing.

The essential components of a USB flash drive comprise a (Oak, 2008):

- male type-A USB connector, which acts as an interface between the device and the computer;
- USB mass storage controller consisting of a tiny RISC processor together with on-chip memory (it can be ROM and RAM);
- NAND flash memory chip which does the actual job of the storage of data; and
- Crystal oscillator, which produces clock signals and controls data output of the device.
The RISC processor or Reduced Instruction Set Computer (RISC) contained on the mass storage controller is a computer arithmetic-logic unit that uses a minimal instruction set, thereby, emphasizing the instructions used most often and optimizing them for the fastest possible execution (Patentdocs, 2007).

The NAND flash memory chip is basically a type of non-volatile storage technology that does not require power to retain data (Tech Target, 2008). NAND is best suited to flash devices requiring high capacity data storage. NAND flash devices offers larger storage space and offers faster erase, write, and read capabilities over NOR architecture (Physorg.com, 2005).

This crystal oscillator component of the flash drive uses a quartz crystal to generate a frequency. Such devices generally output a fixed frequency, but some can be controlled by a tuning voltage over a small range (Answers.com, 2008).

Some of the other components of flash drives include Light Emitting Diodes (LEDs) acting as indicators and write-protect switches (Oak, 2008).

A flash drive, to be operated, has to be inserted into the USB port on the computer. The operating system detects the flash drive and installs the necessary drivers. Some of these operating systems include Windows ME, 2000, XP and Vista. USB drivers are built into the Windows system, except for Windows 98 which requires drivers to be installed for each device. USB drivers are unlikely to be available for Windows 95 and earlier versions (Hogan, 2007).

In the case of Higher Education Institutions using Windows versions released subsequent to Windows 98, it can be assumed that the operating system will detect flash drives that are plugged into computers and will allow students and staff to transfer data between the device and the computer. The small size and large storage capacity of USB Flash Drives can make it a dangerous tool in the wrong hands. As
mentioned, the operating system detects the UFD and will install a driver to enable its use. Users (i.e. students and staff at HEIs) are not required to be a computer administrator to install a UFD and UFDs cannot be managed via Group Policy (Labmice.com, 2003). A computer administrator is a user who manages and maintains a computer. The computer administrator makes system-wide changes to the computer, including installing programs and accessing all files on the computer, allocating disk storage space, adding and configuring new workstations, and he can create, change and delete the accounts of other users (Desepoli, 2008). Group Policy is an infrastructure that allows the implementation of specific configurations for users and computers (Technet, 2003).

It can be deduced that a “normal” user without administrator rights, can plug in a flash drive and transfer data between the drive and any computer on a university campus, because it cannot be controlled through restricting the rights of the user. Conceivably, this poses a major threat to the computing infrastructure of such institutions of higher learning. This statement can be substantiated by expanding the security threats inherent to the use of flash drives as quoted from (Steel-Wargo) in Chapter 1:

- No differentiation between authorized and "rogue" devices:
  Authorized USB devices include keyboards and mice that connect to computers via USB. However, students and staff can plug in UFDs at random and the host computer will simply recognize it as another USB device. There is no way to identify UFDs as “rogue” devices except through implementing additional controls.

- No audit or logging of data on devices:
  A student doesn’t have to be an administrator to connect a flash drive to the USB of a computer and to begin uploading or downloading data of any kind. The student could easily copy the data without any trace because Windows does not take an audit or log that there has been a peripheral device attached to the PC.
• No centralized control:
The fact is that most universities have little or no physical control over the USB flash drives connected to its network. There is no port control or centralized control that would put the access control back in the hands of security personnel. If there were centralized control, if a drive is compromised, lost or stolen, the flash drive could then be terminated instantly with central control.

• Leakage of sensitive data:
There is always the possibility of a USB flash drive containing confidential information being lost or misplaced by accident. A worst case scenario would be a USB flash drive containing exam papers dropping out of the pocket of a staff member.

• Infection from outside data brought into the network on these devices:
Many students use a USB flash drive to transfer files across computers and sometimes from computers outside the university network, hence the USB flash drive can become a carrier of viruses, Trojans, malware and worms. The USB flash drive exploits the computer using the Windows auto run capability that is activated whenever the student plugs in a USB flash drive. Auto run therefore activates the virus and it enters the host (i.e. the computer), which is most likely part of a wider network in the university. Even if the auto run capability is turned off various Trojans or viruses can still be activated or copied onto that computer.

Removing all USB ports of a computer is the only way to be entirely sure that UFDs are not used in a particular environment. In an environment such as a university where each computer’s keyboard and mouse interfaces through USB, this is an impracticable solution. This underscores the need for universities to implement a holistic approach to managing the threats to security due to the use of UFDs.
3.4 Smart Phones

The development of mobile phones can be traced back to the use of two-way radios that were used in vehicles. The first fully automatic mobile phone system, called Mobile Telephone system A (MTA) and weighing 40kg, was developed by Ericson and commercially released in Sweden in 1956 (Wikipedia, 2008). Cell phones would have been mass produced earlier but because the cell phone was held under the two-way radio law the distribution of cell phones was limited.

All matters involved with broadcasting and transmitting either radio or television message in the US, are under the ambit of the Federal Communications Commission (FCC) who regulate that a cellular phone is actually a type of two-way radio (Bellis, 2003). Their decision to limit the cellular phone frequencies in 1947 was revised in 1968, with the FCC stating that "if the technology to build a better mobile phone service works, we will increase the cellular phone frequencies allocation, freeing the airwaves for more mobile phones" (Phone Warehouse, 2000).

Both Bell Laboratories and Motorola were involved in a race to see who could invent the first viable cell phone (Sayush, 2003). In 1973, Martin Cooper, a scientist working for Motorola, successfully made the first ever cell phone call using a portable handset and the age of the cell phone was born (Singh, 2008).

Today's cellular devices are more than just portable telephones. After the initial portable cell phones were released commercially, the race was on to produce smaller and more powerful devices. This led to the age of PDA phones and smart phones.

A PDA (Personal Digital Assistant) is a handheld computer for managing contacts, appointments and tasks. It typically includes a name and address database, calendar, to-do list and note taker, which are the functions in a personal information manager (PC Mag, 2008). The generic term for a PDA oriented device with cellular phone
A smart phone is a mobile phone offering advanced capabilities beyond a typical mobile phone, often with PC-like functionality (Carlton, Kimberly, & Munsey, 2008). There is no industry standard definition of a smart phone. It can be defined as a phone that runs complete operating system software providing a standardized interface and platform for application developers or simply a phone with advanced features (Wikipedia, 2008).

Webopedia (2008) differentiates succinctly between mobile phones, PDAs and smart phones:

- A mobile phone is more frequently called a cellular phone or cellphone. Most mobile phones provide voice communications, Short Message Service (SMS), Multimedia Message Service (MMS), and newer phones may also provide Internet services such as Web browsing, instant messaging capabilities and e-mail.
- PDA is the name given to small handheld devices that combine computing, telephone/fax, Internet and networking features and can typically function as a cellular phone, fax sender, Web browser and personal organizer. These devices are usually pen-based.
- A smart phone is considered to be a combination of the traditional PDA and cellular phone, with a bigger focus on the cellular phone part. These handheld devices integrate mobile phone capabilities with the more common features of a handheld computer or PDA.

The first smart phone, called Simon, was designed by IBM in 1992 and released to the public in 1993 (Wikipedia, 2008). Others like Nokia and Ericsson launched their own series of smart phones soon thereafter.
A smart phone could be best described as a high-end phone with converged PDA features which may include (Jones, 2008):

- Personal information management;
- LAN connectivity;
- Graffiti style data entry;
- Local data transfer between phone set and computers;
- Remote data transfer between phone set and computers;
- Remote control of computers;
- Remote control of home or business electronic systems; and
- Wireless e-mail, Internet, Web browsing, and fax.

The popularity of smart phones has increased over the years. In today's digital age we demand constant connectivity and expect to be as productive out of the office as we are in it. Smart phones not only combine the functionality of a cell phone and a PDA, but also include embedded operating systems, enabling users to use them as a mobile PC (Bearly, 2007). Smart phones are quickly outstripping PDAs as employees turn to multifunctional cell phones to stay organized, connected and entertained at home and at work (Mcadams, 2007).

Having all your contacts and appointments at hand is one of the most convenient things about owning a hand-held organizer, and synchronizing makes it easy to keep both the hand-held and your big computer up to date (Hutsko, 2002). Programs such as Intellisync provides smart phone users with two-way, desktop-based synchronization of email, calendar, contacts, and tasks with popular PC applications such as Microsoft Outlook and Outlook Express, Lotus Notes, Novell GroupWise, ACT (MSMobiles.com, 2004). The synchronization of about 300 contacts and 75 calendar items can take as long as 10 minutes the first time. After the first synchronization, subsequent syncs generally take only a few seconds (Hutsko, 2002). This ease of use
in synchronizing data and transfer of data between mobile devices such as the smartphone and a computer, must again point to the obvious increase in security threats.

Employees can pose risk to an enterprise IT infrastructure through mobile devices such as smart phones and laptops, as well as the various networks and applications with which their unsecured devices are liable to interact (eWeek.com, 2008). In a survey of 300 IT managers conducted by Credant, it was found that most of them saw phones as bigger security threats than company-issued laptops (Miguel, 2008). Other than the pin code, there is no native form of authentication for the most widely used smart phones despite the fact that they are often used for personal or confidential data (Delpha & Rashid, 2004).

In the context of this research, the risks posed by the use of smart phones in a university environment, are similar to the risks posed by UFDs. This is because this research only considers the use of smart phones connecting to the campus computers via USB. Other risks which arise through wireless access, for example, are excluded. Therefore, as with UFDs, the inability to identify such smart phones as “rogue” devices, the lack of log tracking and centralized control, the possible leakage of data and exposure to malicious code are some of the relevant security threats.

Notably, over 500 viruses and other types of malware that specifically target smart phones have already been identified and a steady stream of around 10 new threats are confirmed each week (Charged SA, 2009). Smart phones, like other portable computing devices, are beyond the reach of organizational firewalls and other security measures (Mcadams, 2007).

While it is fairly straightforward for IT departments to manage and secure business applications that reside on company-issued laptops or PCs, doing this on mobile devices – some of which may not be owned by the company – presents a far greater challenge (Bancroft, 2008). Considered together with the increased use of portable
devices such as mobile phones by staff and students in universities (Anderson & Blackwood, November 2004), again the risks posed and the fact that it needs to be addressed, are clear.

3.5 MP3 Players

The world’s first mass-produced hardware MP3 player was Saehan’s MPMan, sold in Asia starting in the late spring of 1998 and released in the United States as the Eiger Labs MPMan F10/F20 (two variants of the same device) in the summer of 1998 (Buskirk, 2005). The original iPod, released in 2001 combined a 5GB hard drive with a rechargeable battery pack and a paradigm breaking user interface—it didn’t necessarily do that much differently under the hood from other MP3 players, but it had a sleek design (by 2001 standards), a unique and simple navigational system, and the Apple brand name to back it all up (Technabob, 2007).

Today Portable Music Player (PMP) devices come in all shapes. Here are some acronyms and explanations (Webopedia, March 2008):

- PMP devices which stands for portable music player devices, is a term used to describe any digital portable music player that allows you to download or save digital music files (in MP3 format) from a computer to play on a PMP.
- An MP3 player is basically a storage device that contains solid-state memory, like flash memory, and players may also include features such as playlists, radio or Web site streaming, and basic options like being able to choose backlight color, and equalization options. MP3 players most commonly use the USB port on your computer for data transfer however some may plug into the FireWire or parallel port. Today there are also a host of other consumer devices which have an embedded MP3 player (e.g. satellite radios, smart phones, PDAs, sunglasses, and even MP3 watches).
Some PMP devices like MP3 players, are also called DAP, short for digital audio player.

Common features of all MP3 players are a memory storage device, such as flash memory or a miniature hard disk drive, an embedded processor, and an audio Codec microchip to convert compressed sound into analog form that is then played through the speaker jack (Wikipedia, 2008).

Although there are many portable music devices due to scope limitations and for the purposes of this dissertation only a technical description for iPods will be given.

iPod combines a major advance in portable music device design with ease of use and Auto-Sync, which automatically downloads all songs and playlists into the iPod, and keeps them up to date whenever the iPod is plugged into the computer (Apple, 2008). The iPod can connect to a PC through a special 32-pin cable to USB-2.0 or FireWire (Philips, 2003).

In terms of size and weight, the 80-GB iPod classic is less than half an inch (1.4 centimeters) deep and weighs about 4.9 ounces (140 grams) versus the Zen Portable Media Center from Creative, which is 1.06 inches (2.7 centimeters) deep, weighs 12 ounces (340 grams) and has only 20 GB of hard drive space (Layton, 2008). The current highest-capacity iPod is 160GB, and is advertised as being able to hold 40,000 songs (Rosoff, 2008).

In terms of using the iPod, when plugged into the PC it appears to the computer as a removable storage device - basically as an external hard drive. In fact, media files are copied to the device as an external hard drive, and the iPod’s database is accessed directly and updated with the information contained in it using normal file access methods (Hollington, 2008).
Threats relating to iPods and other MP3 players range from the introduction of copyrighted media onto the corporate (or campus) network for which the company or institution becomes liable, to the theft of business critical data, to the introduction of malicious code which could be accidental or an intended act of sabotage (Sturgeon, 2005). In the university environment students could ostensibly be listening to music, while they are copying and viewing copyrighted media using the campus computing infrastructure.

3.6 Conclusion

Mobile devices are likely to converge into a hybrid of smart phone, PDA and media technologies, which can be termed a PACE (Personal Assistant, Communication and Entertainment) device (Anderson & Blackwood, November 2004). Whilst there is a strong trend towards convergence between classes of device, it is difficult to predict whether the end point will be a single appliance or a range of devices offering differing subsets of technologies (Sharples & Beale, 2003). It is quite possible to predict though, that over the coming years increasing numbers of students will be presenting a variety of mobile devices and will expect to be able to use them within the university network infrastructure (Anderson & Blackwood, November 2004). It can further be concurred that technological ‘ease of access’ always pre-empts security and that the lag is, naturally, exploited vociferously (Charged SA, 2009).

From the corporate point of view, security analysts are encouraging companies to consider banning portable storage devices such as UFDs, smart phones and Apple's iPod from corporate networks, as they can be used to introduce malware or steal corporate data (Donoghue A., 2004). From the higher education point of view, portable storage devices are seen as presenting education with a number of opportunities to enhance learning, administration and research, but also presents new challenges for the management and support of university infrastructure (Anderson &
In this chapter it was shown how portable storage devices have become more available, and although are technically complicated, are relatively easy to use. This ease of use presents major security risks as these small and non-obvious devices can become weapons in the hands of its users. As previously mentioned, this requires appropriate controls to be implemented in order to protect the environment. In Chapter 4, this requirement, namely to protect the environment, is broached through the proposal of a framework for the secure use of portable storage devices.
“It is becoming harder to keep track of security issues and how to defend yourself. Once you build a better mousetrap, hackers build better mice. But companies can do more to protect themselves.”

Lance Hayden
Cisco Secure Consulting Services group
4.1 Introduction

A framework is an underlying a set of ideas, principles, agreements, or rules that provides the basis or outline for something intended to be more fully developed at a later stage (MSN Encarta, 2008). In this Chapter, a framework for the secure use of portable storage devices at SA HEIs is proposed. The purpose of the framework is to enable HEIs to consider security in regard of the use of portable storage devices in their environments, in a holistic and systematic way. The various parts of the framework ensure that all aspects that are addressed, fit in with the rest of the framework in a logical way. The framework is triangular and suggests an outline for security measures to ensure the secure use of PSDs.

The framework is depicted graphically in Figure 4.1. It is divided into three layers namely:

- A dictating top layer called “By Order”, indicating that it takes an instructive stance in the context of the framework;
- A people-oriented middle layer called “By Behaviour” which recognizes that security is only as strong as the people who are involved; and
- A technical bottom layer called “By Technology” which provides a guideline for the information technology security products that must be implemented to secure the environment.

The framework is discussed in greater depth in Section 4.2. The three layers comprising the framework are discussed in Sections 4.3 – 4.5 and the Chapter is concluded in Section 4.6.
Figure 4.1: A Triangular Framework for the Secure use of Portable Storage Devices
4.2 A Framework for the Secure Use of Portable Storage Devices at South African Higher Education Institutions

Each of the layers of the framework depicted in Figure 4.1, depicts the categories to be addressed within the ambit of the particular layer.

The top layer entitled “By Order” provides a directive to guide the implementation of security. It deals with matters of a compulsory nature, i.e. legal and policy requirements as well as the use of standards.

The middle layer of the framework entitled ‘By Behaviour’ refers to the people involved in the higher education environment, either as users (students) or as staff. It requires proper security education, training and awareness (SETA) to ensure that an informed body of students and staff execute the directives received “by order” (i.e. from the top layer of the framework).

The bottom layer of the framework entitled ‘By Technical’ forms the basis of the framework in providing the IT security solutions to support the people (middle layer) in the execution of the instructions (top layer) to secure the environment.

In Sections 4.3 – 4.5 each of the layers and categories are discussed in detail. The discussion takes the format of a theoretical introduction of the layer-category combination and ends off with an example that demonstrates its application at a fictitious South African Higher Education Institution.

4.3 The “By Order” Layer

This layer of the framework is divided into three categories namely: Laws, Standards and Policies. Each of these categories is subsequently discussed.
4.3.1 Laws

The role of the Laws category in the context of this framework is to ensure legal compliance.

Laws, according to the business dictionary, are a binding set of rules of conduct whether written or not and are meant to enforce justice and prescribe duty or obligation. Laws are generally derived from custom or formal enactment by a ruler or legislature (BusinessDictionary).

In the South African context, there are various legal instruments that are of relevance and will be briefly discussed here. One of the main cyber laws in South Africa is the Electronic Communications and Transactions Act (ECTA). The ECT Act is one of many sources of law which impact on electronic communications and transactions and must not be read in isolation of relevant statutory and common law. It applies to any form of communication by e-mail, the Internet, SMS, etc. except for possibly voice communications between 2 people (Michalsons, 2005).

The main objectives of the ECTA include (ECTA, 2002):

- To provide 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 the abuse of information systems;
- To encourage the use of e-government services; and
- To provide for matters connected therewith.
Other South African laws that address cyber crimes include:

- The Prevention of Organized Crime Act (POCA);
- The Financial Intelligence Center Act (FICA);
- The Films and Publications Act No.65 of 1996. The aim of the Films and Publications Act, in its present form, is to allow adults the maximum amount of freedom, while simultaneously protecting children against material that is harmful (Buys, 2003).
- The Promotion of Access to Information Act (PAIA). PAIA was enacted in 2000 to give effect to Section 32 of the Constitution of the Republic of South Africa (Act 108 of 1996), that allows every South African access to information held by public and private bodies (Buys Inc Attorneys, 2008).
- Exchange control regulations. Money laundering and other financially related crimes which are done electronically or digitally may contravene exchange control regulations (Madziwa & Snail, 2008).

There are some international laws that are relevant because of the Internet expanding the reach and area of operation of businesses globally. The Sarbanes-Oxley Act, referred to as SOX or SOA, was passed by the United States / American Congress in July 2002 to improve regulatory visibility and accountability of public companies. This legislation was enacted largely due to corporate accounting scandals typified by Arthur Anderson, Enron and WorldCOM (Hong Kong Government, 2008). SOX is based in the United States (US) but it applies to global companies trading in the US.

Without a doubt, laws are a compulsory aspect of any framework for security. The laws mentioned in this section (and other laws) must be complied with (where relevant) and therefore South African HEIs must take this into account in terms of securing their environments. In Figure 4.2, the Laws category of the “By Order” layer of the framework is illustrated through the use of an example in a fictitious HE environment (University XYZ).
Student A copies hacking software or malicious code using a flash disk. The student plugs his flash disk into a USB port and copies the malicious code onto a PC at University XYZ with the intention of causing harm.

The Electronic and Communications and Transactions Act states that a person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilize such item to contravene this section (of the Act), is guilty of an offence.

University XYZ has a policy document stating that it subscribes to the principals of the ECT Act and students sign this document when they join the University. The university also has a procedural agreement with terms and conditions on the log-on page of the pc’s which have to be accepted before usage. The institution has a legal obligation to protect information according to the ECT Act. If the University can show due care in implementing security measures, it has legal recourse against the student if damages were suffered due to the particular incident.

Figure 4.2: Example – Layer: “By Order”, Category: Laws
4.3.2 Standards

In the context of this framework, the role of the Standards category is to ensure that accepted best practices are followed.

Standards are really anything that applies a definite rule, principle, or measure established by an authority (Merriam-Webster, 2008). For example, standards can define the scope of security functions and features needed for the following (Stallings, 2007):

- Policies to manage information and human assets;
- Criteria for evaluating the effectiveness of security measures;
- Techniques for the ongoing assessment of security and for the ongoing monitoring of security breaches; and
- Procedures for dealing with security failures.

Relevant examples of information security standards / best practices are subsequently discussed.

The International Organization for Standardization (ISO) is a well known standardization body. The ISO has developed over 17000 International Standards on a variety of subjects and 1100 new ISO standards are published every year (International Standards for Organizations, 2008). The ISO is a non-governmental body which promotes the standardization of developments globally.
Two of the prominent information security standards published by the ISO and adopted by the South African Bureau of Standards, are:

- ISO/IEC 27001: 2005 *Information Technology Security Techniques Information Security Management Systems Requirements*, which specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization’s overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof (ISO/IEC 27001, 2005). It covers all types of organizations for example, commercial enterprises, government agencies and not-for-profit organizations.


The ISO 27002 advises companies on what means and methods they should employ to ensure that their Information Security Management is effective (Von Solms & Von Solms, 2008). It provides best practices for control objectives and controls in the following areas of information security management (Arnason & Willett, 2008):

- Security policy;
- Organization of information security;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
• Access control;
• Information systems acquisition, development and maintenance;
• Information security incident management;
• Business continuity management; and
• Compliance.

An example of a best practice that is used for IT governance is COBIT 4.1. It provides a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks (Cambinet, 2008). COBIT divides IT Governance into 34 high-level IT processes. These high-level processes are divided further into four domains namely:

• Plan and Organize;
• Delivery and Support;
• Acquire and Implement; and
• Monitor and Evaluate.

Each domain has several processes. Under Delivery and Support is a process entitled "Ensure System Security". This is the link between COBIT, which is IT governance based and information security. The process is called DS5 and it is one of 13 other processes in that domain (Von Solms & Von Solms, 2008). Although DS5 relates directly to information security, there are other processes which are more indirectly security related such as DS4 which is a high-level process which Ensures Continuous Service and it addresses the existence of a proper IT continuity plan. Another control objective which is indirectly related to information security is PO2 which falls under the domain Plan and Organize. The process PO2 defines the Information Architecture.

In Figure 4.3, the discussion of the Standards category of the “By Order” layer of the framework, is contextualized by expanding the example based on University XYZ.
University XYZ implemented the ISO 27002 in order to ensure due diligence in the protection of its information assets. This will ensure that it complies with the legal obligation (e.g. from the ECT Act) to protect its information. Section 10.4 of the standard addresses ‘Protection against malicious and mobile code’. It suggests controls and implementation guidance to achieve the objective of protecting the integrity of software and information. The University implemented these controls including a network scanning PC which detects if there is any malicious code on the network, antivirus software and additional malicious code prevention software. Daily updates of definition files and scanning engines are made keeping them up to date.

Because of the controls that were implemented, the incident was recognized and the malicious code quarantined and deleted. Therefore the issue was resolved before much damage had been inflicted.

Figure 4.3: Example – Layer: “By Order”, Category: Standards
4.3.3 Policies

The role of the Policies category is to ensure that organizational guidance is provided to ensure that security objectives are met. Policies are generally of a directive nature and therefore resort in the “By Order” layer of the framework.

Corporate-level policies are normally formulated by a board of directors. These policies direct and restrict the plans, decisions, and actions of organizational stakeholders in the achievement of the organization’s objectives (Business Dictionary, 2008). The purpose of security policies is to outline security-related responsibilities within the context of an organization’s legal obligations. Secondly it provides a tool to measure policy compliance and thirdly, provides an indication of acceptable and unacceptable behaviour as well as penalties where relevant. It is therefore clear that an organization cannot approach security without implementing proper and extensive information security policies.

In Figure 4.4, the Policies category of the “By Order” layer of the framework, is illustrated using an example.

4.4 The “By Behaviour” Layer

This layer of the framework is divided into three categories namely: Awareness, Education and Training. The NIST SP800-50 defines these concepts in the following way (NIST, 2007):

- Awareness assists in focusing attention on security;
- Training helps to produce relevant and needed security skills and competencies; and
University XYZ implements a computer lab usage policy. The policy mentions some rules and regulations for using lab computers. It also mentions that the university is subscribed to the principles of the ECT Act and any unlawful behaviour would be dealt with according to the policy. The policy also has an agreement side to it which mentions that whoever signs the agreement is bound by the clauses in the agreement.

When Student A joined University XYZ, he had to sign the computer lab usage policy in order to be able to use the labs. When Student A unlawfully committed the act of copying malicious code onto the network, this brought the conditions stated by the Lab Usage Policy into play. Fortunately not much damage was caused by the incident and therefore Student A only had his account disabled.

Figure 4.4: Example – Layer: “By Order”, Category: Policies

- Education assists to integrate all (security skills and competencies) into a common body of knowledge, adding a multidisciplinary study of concepts, issues, and principles.

Each of these categories is subsequently discussed in Sections 4.4.1 – 4.4.3.
4.4.1 Awareness

The role of the *Awareness* category is to ensure that users are aware of security policies, security issues and their role in the matter. Security awareness efforts are designed to change behaviour or reinforce good security practices (NIST, 2007).

Information security management needs, at a minimum, the participation by all the employees in the organization (InfoSecurityLab, 2008). The best way to achieve a significant and lasting improvement in information security is not to attempt ever-increasing technical solutions but to raise awareness among the users who interact with the computer networks, systems, and information in the basics of information security (Native Intelligence, 2008). A robust and enterprise wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them (Newell, 2008).

The NIST Special Publication 800-50 which was referenced at the start of Section 4.4 to define the concepts of security education, training and awareness (SETA), is a widely known standard which addresses security awareness and training in particular, in more detail. It provides best practices for building and maintaining a comprehensive awareness and training program as part of the IT security program of an organization. A distinct difference is made between the concepts of awareness and training. The purpose of awareness is simply to focus attention on security. Awareness presentations, for example, are intended to allow individuals to recognize IT security concerns and respond accordingly (NIST, 2007). The purpose of training as explicated by the NIST SP800-50, is discussed in Section 4.4.3.
In Figure 4.5, the *Awareness* category of the “By Behaviour” layer of the framework, is illustrated in relation to the example of University XYZ that has been used in this Chapter.

**Figure 4.5: Example – Layer: “By Behaviour”, Category: Awareness**

*University XYZ has implemented a security awareness campaign using posters, email, websites, presentations, etc. Student A, although having been made aware of the rules in regard to malicious code, chose to ignore it and therefore the consequences stated in the Computer Lab Usage Policy were enforced.*

**4.4.2 Education**

Education is achieved through theoretical instruction and is for individuals who want to further their understanding in information security – it is a long term solution to information security (Von Solms & Von Solms, 2008). The role of the *Education* category in the context of this framework is to ensure that Universities consider or investigate the integration of information security as a component of formal academic programmes. This can be customized to the particular qualification (e.g. an undergraduate degree in Computer Science versus...
a post-graduate Certificate in Information Security Governance versus an undergraduate Diploma in Marketing). In this way, the University will contribute to creating a workforce where:

- Information security literacy is established as part of formal academic programmes and integrated into the student’s discipline of study; and
- Information security knowledge and expertise forms an integral part of academic programmes where the computing discipline forms a sizeable part of the qualification.

In Figure 4.6, the University example is extended to illustrate the *Education* category of the “By Behaviour” layer of the framework.

*University XYZ*                                        *ICT Staff Member*                            *Postgraduate Certificate: Information Security Governance*

University XYZ, recognizing the need to develop capacity in the area of Information Security Governance, decided to sponsor one ICT staff member annually to complete a Postgraduate Certificate in Information Security Governance.

**Figure 4.6**: Example – Layer: “By Behaviour”, Category: *Education*
4.4.3 Training

Training is a needs-driven process that is typically directed to the learner by an organization. The role of the Training category is to ensure that the University trains ICT staff (either internally or externally) to have the necessary technical skills and competencies related to information security. The need for training will usually be driven by the organization and not by the learner.

The organization identifies a situation where the learner is required to attain new skills or behaviors supporting skills (Sapieha, 2007) and arranges for the necessary training to take place.

According to NIST Special Publication 800-50, the most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual’s attention on an issue or set of issues (NIST, 2007). An example of a training course relevant to the domain of information security is the ISO/IEC 27001:2005 - Understanding an Information Security Management System (ISMS) two day course as advertised by the BSI Group. This course provides an overview of the latest techniques and examines issues surrounding an ISMS (ISO/IEC 27001, 2005).

The Training category of the “By Behaviour” layer of the framework is illustrated in Figure 4.7.
4.5 The “By Technology” Layer

The selection of IT security products is an integral part of the design, development and maintenance of an IT security infrastructure that ensures confidentiality, integrity, and availability of mission critical information (NIST, 2003). The purpose of the “By Technology” layer of the framework is therefore to ensure that the necessary IT security products are implemented to secure the environment.

A good guideline to choosing the right technology for securing information is NIST Special Publication 800-36, entitled Guide to Selecting Information Security Products.
This guide defines broad security product categories and specifies product types within those categories (Grance, Stevens, & Myers, Guide to Selecting Information Technology Security Products, 2003). The “By Technology” layer of the framework is divided into nine categories which denote IT security product categories as identified by the NIST SP800-36, viz. (NIST, 2003):

- Identification and authentication;
- Access control;
- Intrusion detection;
- Firewalls;
- Public key infrastructure;
- Malicious code protection;
- Vulnerability scanners;
- Forensics; and
- Media sanitizing.

In terms of the framework, these IT security product categories constitute the technological foundation of a secure higher education computing infrastructure. Each of the categories is discussed briefly in Sections 4.5.1 – 4.5.9.

### 4.5.1 Identification and Authentication

Identification is the process whereby an element recognizes a valid user's identity, whereas authentication is the process of verifying the claimed identity of a user (Olsen, 1995). Authentication processes can contribute to the protection of privacy by reducing the risk of unauthorized disclosures, but only if they are appropriately designed given the sensitivity of the information and the risks associated with the information (ITU Corporation, 2006).
4.5.2 Access Control
Access Control is any mechanism by which a system grants or revokes the right to access some data, or perform some action. Normally, a user must first log into a system, using some authentication system (Hitachi, 2009). Thereafter the allocated rights (via the access control mechanism) will apply to the user.

4.5.3 Intrusion Detection
Intrusion detection is a type of security management system for computers and networks. An intrusion detection system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches (TechTarget, 2009). It takes a proactive approach to identifying security violations thereby limiting possible damage to the IT infrastructure.

4.5.4 Firewall
Firewalls are recognized as a primary method to keep computer networks secure from intruders. A firewall allows or blocks traffic into and out of a private network or the user's computer. Firewalls are widely used to give users secure access to the Internet as well as to separate a company's public Web server from its internal network. Firewalls are also used to keep internal network segments secure (PC mag, 2009). For example, many corporate enterprise intranets employ firewalls to restrict connectivity to and from internal networks servicing more sensitive functions, such as the accounting or personnel department (NIST, 2003).

4.5.5 Public Key Infrastructure
A public key infrastructure (PKI) is a foundation on which other applications, systems, and network security components are built. It is an essential component of an overall security strategy that must work in concert with other security mechanisms, business practice, and risk management efforts (Weise, 2001). A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private
4.5.6 Malicious Code Protection
Malicious code protection requires strict procedures and multiple layers of defense (NIST, 2003). Malicious code is any program that acts in unexpected and potentially damaging ways. Common types of malicious code are viruses, worms, Trojan horses, monitoring programs such as spyware, and cross-site scripts. (Federal Financial Institutions Examination Council, 2008). Malicious code protection is necessary to protect IT Systems from damage caused by malicious code.

4.5.7 Vulnerability Scanners
The goal of running a vulnerability scanner is to identify devices on the network that are open to known vulnerabilities (Bradley, 2008). Vulnerability scanners contain a database of vulnerability information, which is used to detect vulnerabilities so that administrators can mitigate through network, host and application-level measures before they are exploited (NIST, 2003).

4.5.8 Computer Forensics
Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence for use in incidents of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud (Robbins, 2008).

4.5.9 Media Sanitizing
Media Sanitizing is a general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means (Kissel, Scholl, Skolochenko, & Li, 2006).
The “By Technology” layer of the framework is illustrated in Figure 4.8 using an example based on University XYZ.

Student A logs onto one of the PCs in a computer lab at University XYZ. To do this the student must be identified and authenticated and therefore logs in with a username and password. The student then plugs his flash drive into the USB port of the PC. Student A proceeds to copy files from his flash drive to his home drive which is a designated drive on a server with space for students to copy their work onto. The student without being aware copies malicious code as part of the data copied onto his home drive.

Although the student is unaware of the malicious code being copied onto the network, the network administrator is made aware by an alert message sent by the vulnerability scanner. The University had implemented a vulnerability scanner which detected that Student A was copying malicious code onto the network and hence the network administrator received a message.

The administrator could therefore find student A where the student was attempting to log in and assist the student.

Figure 4.8: Example – Layer: “By Technology”
The layers and categories of the framework are interrelated and must work together to secure the environment. This implies that it is a combined approach applying various controls addressing different dimensions (e.g. policies vs technical controls) to ensure that people and technology work together to achieve a common goal set by the University, namely to protect its assets.

4.6. Conclusion

In this chapter a triangular framework with three layers contributing to the secure use of portable storage devices was introduced. Each of the layers represents an important yet individual aspect of creating a secure infrastructure that can accommodate the secure use of portable storage devices. It is important to realize that each layer must function concomitantly with the other two layers. Only by using all three layers together will the framework be fully effective in the sense of ensuring a holistic approach. For example, a training programme (middle layer of framework) addressing a very specific technical skill (e.g. the use of a vulnerability scanning product) can be seen as resulting from the implementation of a vulnerability scanner (bottom layer of framework) which was identified as a requirement through the adoption of a particular security standard (top layer of framework).

In Chapter 5, the research is concluded by revisiting the research process and the output (i.e. the proposed framework) that was presented in Chapter 4.
“If you're smart, you're concerned about computer security. Open ports on your computers are invitations to criminal hackers and other evildoers to wreak havoc - and if you don't protect yourself, no one else will.”

Jason Thomas
5.1 Introduction

In this chapter the research reported on in the dissertation, is concluded. Chapter 5 provides an overview of how the objectives of the research were met in each chapter. The benefits and limitations of the research are considered and suggestions made as to how the research can be extended in the future.

At the start of this dissertation, the South African Higher Education landscape was introduced as being in a state of flux. One of the reasons for this is the merger process that was forced upon South African Higher Education Institutions. Due to the mergers universities experienced massive infrastructure growth and ended up with widely distributed computing infrastructure. This means that not only did the number of computers attributable to one institution increase, but computer labs are dispersed across geographic areas which makes it harder to control and protect.

At the same time, the South African government is increasing funding allocations to these institutions, inter alia to develop the technological skills of students who are being educated to enter the world of work, to contribute to the economy of the country. Thus, universities are experiencing an increase in the number of techno-savvy students. Furthermore, many students today own portable storage devices, mobile phones and/or MP3 players for their personal use or for educational purposes within the institution. Many of these devices have the ability to connect to a PC via USB to upload or download data.

Most computers nowadays are fitted with a USB connection because of its ease of use and how fast it is to connect peripheral computer devices such as printers, modems, speakers, cameras etc. Considering that campus computer laboratories are equipped with computers that need USB connections for the keyboards and mice, it follows that these peripheral devices can be used in and connected to the computers in these labs. This exposes the university computing infrastructure to various threats.
This research focused on storage devices that have mass storage capacity combined with portability and the capability of being connected to a USB connection. Mass storage capacity allows students and staff to copy or store large files such as multimedia files (music or videos), PowerPoint presentations, etc. on one device. It also allows one to transfer large amounts of data between devices, including PCs. Students and staff can work from computers that are not necessarily part of the universities’ network, for example, to complete assignments, projects or homework at an off campus location. Portable devices with large storage capacity, facilitate the easy transfer of work when continuing with such work at university.

Where in the past a floppy disk was used to copy homework or documents, today flash drives, phones, PDAs and various other devices are used. Nearly all peripheral devices available today have a USB option of connection. PCs generally do not have floppy drives but rather have USB connections.

Smart phones, MP3 players and USB memory sticks are typically enabled for USB connection and pose a real risk for higher education institutions. These risks vary from personal information getting into the wrong hands, loss of data, slurping, to malicious code and so forth. The innocent action of plugging in a mass storage device into a USB port of a PC could for example result in infection from viruses, or allow for illegal material or unlicensed software to be transferred between the device and the PC, which could be connected to the broader network of a university.

The extent to which the use of devices such as flash drives and MP3 players put the university at risk, is underscored by the following statements by Brooks (2005):

“The more portable a device, the easier it is to lose—whether by accident or malicious intent. In any case, the digital booty can range from one person’s list of bank passwords to a spreadsheet containing the Social Security numbers and other personal information of tens of thousands of students—
as the University of California, Berkeley, demonstrated a few months back when such a list became publicly available.”

Therefore, this research investigated countermeasures that contribute to mitigating the risks posed by portable devices such as USB flash drives, smart phones and MP3 players and proposed a solution in the form of a triangular framework. The framework suggests an outline for security measures to ensure the secure use of these devices at South African Higher Education Institutions. This then addressed the primary objective of the research as stated in Chapter 1:

The primary objective of this research project is to create a framework for the secure use of portable storage devices in South African Higher Education Institutions.

5.2 Chapter Overview

In order to meet the primary objective of this research, a number of sub-objectives were identified in Chapter 1. This section shows how the sub-objectives of the research were met on a “per chapter” basis.

5.2.1 Chapter 1 – Introduction

Chapter 1 highlighted the state of the higher education sector in South Africa. The increasing use of portable storage devices at universities was mentioned and the resultant risks that must be managed in order to protect the environment. This led to the formulation of the problem statement, objectives and the methods used in meeting the objectives of the project.
5.2.2 Chapter 2 – The South African Higher Education Landscape

**Sub-Objective 1**
Investigate recent changes in the South African higher education landscape and the use of technology at Institutions of Higher Learning.

**Research Question**
How has the higher education sector changed in South Africa and how have Institutions of Higher Learning adapted to incorporate technology in their environments and teaching practices?

The chapter commenced by introducing the South African education system, showing statistics regarding the number of learners and schools at primary and secondary level and the number of students, Universities and Technikons at tertiary level. The governance structures of the education system were explained including statutory bodies and laws that regulate the higher education sector. An overview of the changes and transitions faced by higher education institutions was provided. The higher education landscape after the mergers was reviewed. It was concluded that the mergers had various negative effects and that in political circles at least, the possible review of merged institutions has been mentioned.

The second part of Chapter 2 investigated the role of Information and Communication Technologies in education in South Africa. Infrastructural limitations and lack of Internet access were shown as being barriers to the use of ICTs to support teaching and learning, although South Africa is favorably positioned in regard of ICT infrastructure as compared to its African counterparts. Notwithstanding infrastructure issues, it was shown that in South Africa the contribution (and potential contribution) of ICTs to economic and educational goals are well recognized and accepted.
5.2.3 Chapter 3 – Portable Storage Devices

**Sub-Objective 2**
Determine the origin and evolution of portable storage devices and consider how their use in higher education institutions is increasing the risk of harm to computing facilities;

**Research Question**
How have portable storage devices developed in recent years and which risks are posed through the use of these devices in higher education institutions?

In Chapter 3 the term Universal Serial Bus and its use to connect peripherals to a PC, were explained. Portable devices with mass storage capacity and that can connect to a PC via USB, were listed as the focus of this research. These comprise USB flash drives, smart phones and MP3 players. Anderson and Blackwood (2004) were quoted as confirming the widespread adoption of mobile devices by students with an expected increase in their use within university network infrastructures in the future.

The Chapter provided a historic overview and technical description of each of these three types of devices and ended off by considering the security threats inherent to the use of the devices. The Chapter concluded that while the use of portable devices like USB flash drives should be discouraged in corporate environments, they are seen as enablers for teaching and research in the higher education environment and their use can therefore not be precluded. The resultant increase in risk to campus computing infrastructures and the subsequent need to implement proper controls, were recognized.
5.2.4 Chapter 4 – A Framework for the secure use of Portable Storage Devices at South African Higher Education Institutions

**Sub-Objective 3**
Examine the countermeasures that are available to mitigate the risk of using portable storage devices in higher education institutions

**Sub-Objective 4**
Create a framework for the secure use of portable storage devices in South African higher education institutions, which incorporate the required countermeasures

**Research Questions**
- How can the increasing risk of possible harm to the computing facilities through the use of portable storage devices, be countered?
- Can the countermeasures to ensure secure use of portable storage devices in South African higher education institutions, be conceptualized in a framework to serve as a guideline for these institutions?

Chapter 4 commenced with a high-level overview of a proposed framework for the secure use of portable storage devices at SA Higher Education Institutions. The framework consists of three layers, each comprised by various categories. The layers and categories together provide an outline for the countermeasures that, when implemented, will mitigate the increasing risk to university computing facilities as a result of the use of portable storage devices. The chapter provided a scenario or example to illustrate each layer / category combination of the framework, in the context of a higher education institution, viz. University XYZ.
5.2.5 Chapter 5 - Conclusion

The research project is concluded in this chapter. The research objectives and research questions were discussed in the context of the chapters of the dissertation, showing how the objectives were reached.

The last part of this chapter will review the benefits and limitations of the research and propose future research directions.

5.3 Benefits and Limitations of the research

The main benefit of this research is that it provides a holistic framework which outlines an integrated approach to securing campus computing facilities, from the point of view of portable devices and their use in this environment.

The main limitation of the research is that it focuses on selected portable devices, i.e. devices with mass storage capacity and with the ability to connect to a PC via USB. Specifically only USB flash drives, smart phones and MP3 players were considered. Therefore the framework, while it may be more broadly applicable than for the selected portable devices, it was not created with devices and threats other than those mentioned in mind.

Secondly, the framework postulates a theoretical solution. The solution is therefore not verified except through the provision of fictional scenario descriptions, which were provided as examples rather than for verification of the solution. The researcher’s work experience at the ICT Services Division of a University, at most contributed to his understanding of mergers, students, staff and the use of portable storage devices in that particular environment. However, it fell outside of the scope of this study to test the solution at a Higher Education Institution and it is conceded that this is a weakness from a research point of view.
5.4 Future Research

Based on the fact that the framework was not tested in a particular higher education environment, it makes sense that the following research activities can be proposed:

- Develop a checklist, based on the framework, to determine to what extent an Institution complies with the proposed framework;
- Monitor the environment and compile a database of security incidents related to the use of PSDs over a period of time;
- Analyze the incident database and the severity of damage caused;
- Based on the results of the analysis, propose changes to the framework to include more layers and / or categories which will ensure that the incidents and the damage caused, are limited to an acceptable level;
- Extend the framework beyond its current scope of selected portable devices.

5.5 Conclusion

At the conclusion of this research project, it is appropriate to reflect on the perspectives gained from various secondary data sources referenced in this dissertation. It was established that the Higher Education sector is a sector in flux due to various reasons, but fuelled to a large extent by the mergers of various Higher Education Institutions. It was shown that the benefits of the use of ICTs at Institutions of Higher Learning is recognized and encouraged, for example, through the provision of funding by the South African government. It was further shown that the use of portable devices at Institutions of Higher Learning is growing in popularity and that students themselves are becoming more technologically proficient. The fact that there is an increase in risk to campus computing facilities due to these factors, was established. This led to the proposal of a framework to outline the countermeasures that will contribute to mitigating these risks.
In this chapter, it was illustrated that the research objectives that were established at the beginning of the research project, were accomplished. The information covered in the different chapters of the dissertation was reviewed and ideas for future research were suggested.

The future may present Institutions of Higher Learning with even greater challenges due to the continued increase in students using mobile devices. As mentioned, these devices are seen as presenting an opportunity to be explored in terms of its potential to contribute to teaching and research. These devices are intelligent and wireless-enabled and Universities may have to make a significant paradigm shift away from supporting a lab-based PC infrastructure to supporting wireless access to the network from a student's own hardware (Anderson and Blackwood, 2004).
References


Brown, L. (2007). Challenges and Opportunities. Information literacy skills training of staff and students in the Unisa Library, 4-5.


National Research Foundation. (2004). *A National Key Research and Technology Infrastructure Strategy*. *Department of Science and Technology*


Gaithersburg: NIST Special publications.


