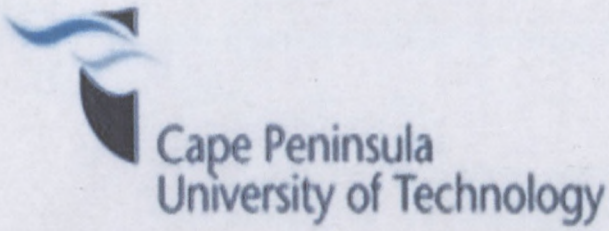
SECURITY CONSIDERATIONS OF e-LEARNING IN HIGHER EDUCATION INSTITUTIONS

TABISA NCUBUKEZI



SECURITY CONSIDERATIONS OF e-LEARNING IN HIGHER EDUCATION INSTITUTIONS

by

TABISA NCUBUKEZI

208217673

Thesis submitted in fulfillment of the requirements for the degree

Master of Technology: Information Technology

in the Faculty of Informatics and Design

CAPE PENINSULA UNIVERSITY OF TECHNOLOGY

Supervisor: Professor N.W Mlitwa

Cape Town

November 2012

DECLARATION

I, Tabisa Ncubukezi, declare that the contents of this thesis represent my own unaided work, and that the thesis has not previously been submitted for academic examination towards any qualification. In addition, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

Signed _____ Date 13/ 11 / 2012

ETHICS STATEMENT

The fieldwork of this study followed Cape Peninsula University of Technology (CPUT) guidelines on the research ethics. The research involved people as study subjects. I (the researcher) was fully aware of the necessary ethical considerations. The data collection process conducted and completed in accordance with the research guidelines. This thesis kept the participants anonymous and their responses confidential.

THESIS SUMMARY

Learning management systems (LMSs) have become the central aspects of educational processes in modern universities. Arguments are that LMSs improve educational efficiencies including the processes of storage, retrieval and exchange of content without distance, space and time constraints. A trusted platform without undue intrusions however, determines the extent to which these benefits can be realized in higher education (HE) spaces. The underlying assumption in this thesis therefore, is that e-Learning systems would lose its value and integrity when the security aspects are ignored.

Despite this logic, an overwhelming evidence security omissions and disruptions continue to threaten e-Learning processes at CPUT, with a risk of the actual usage of LMS in the institution. For this reason, this study sought to investigate the extent as well as causes of existing security threats, security awareness programmes and the in/effectiveness of security measures within CPUT. Within the qualitative interpretive research framework, the purposive sampling method was used to select participants. Semi-structured interviews were then used to collect primary data from administrators, technicians, academics and students in the IT and the Public Relations departments at CPUT. The activity theory (AT) was then used as the lens to understand the security aspect in e-Learning systems in the CPUT. From this theory, an analytical framework was developed. It presents holistic view of the security environment of e-Learning as an activity system composed of actors (stakeholders), educational goals, rules (in the form of policies, guidelines and procedures), activities, mediating factors, transformation, and outcomes. The tension between these components accounts for failures in e-Learning security practices, and ultimately in the e-Learning processes.

Whilst security measures exist on the e-Learning platform, findings show a combination of the tools, processes and awareness measures to be inadequate and therefore inhibiting. Poor adherence to security guidelines in particular, is a major shortfall in this institution. To this end, a continuous review of network policy, clear and consolidated communication between stakeholders as well as emphasis on the enforcement of security compliance by users across all departments is therefore recommended. Frequent security awareness and training programmes for all LMS users must also be prioritized in this institution.

Keywords: e-Learning, LMS, Security, Higher Education Institution.

DEDICATION

I dedicate this work to my special daughter Bongeka Ntombi, and my siblings Lunje, Mpendulo and Mbuzeli. I have set a mark, which I hope you will do well to surpass

ACKNOWLEDGEMENTS

I would like to thank the Lord Almighty for the great work, everlasting love and kindness. His grace has been with me through hard times of my study.

My appreciation goes to Professor Mlitwa, my supervisor for his supervision, guidance to enable me to complete this work. I have insufficient words to thank him for his enthusiasm, patience on systematic procedures and efforts of explaining things more clearly and simply. He has been so helpful throughout the thesis writing.

I would like to thank Ann Bytheway for the tremendous help towards the success of this work.

I gratefully thank the group of Masters Students for their support and encouragement.

My special thanks go to my colleagues at CPUT for assisting and supporting me to do my research while lecturing at the same time.

I would like to thank my parents Khumalo and Ndlovu for bringing me up; I would have not been here without you. Thank you once again for the wonderful work.

Thank you to my spiritual parents (Pst Thom & Thembi Thamaga) and friends for the encouragement, support and prayers at Without Walls Christian Family Church.

My sincere gratitude goes to my special daughter Ntombi Bongeka for allowing me to finish this work.

To my siblings thank you for the words of encouragement, support and prayers in the process.

Thank you to my sister Babalwa, for the inspiration, care and prayers.

Lastly thank you to everyone for positive contributions towards this work.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

Acronym	Meaning
A	Accessible
AT	Activity Theory
CPUT	Cape Peninsula University of Technology
CTS	Computer and Telecommunication Services
DoS	Denial of service
E	Efficient
e-Learning	Electronic Learning
F	Flexible
FID	Faculty of Informatics and Design
HE	Higher Education
HEI	Higher Education Institution
ICT	Information and Communication Technology
IS	Information Systems
IT	Information Technology
KEWL	Knowledge environment for Web based learning
LMS	Learning Management Systems
PR	Public Relations
S	Security
SA	South Africa
UWC	University of Western Cape

CHAPTER ONE: INTRODUCTION

1. Introduction

The adoption and use of technology to support teaching and learning in higher education institutions has grown significantly since the turn of the 21st century. Through the use of learning management systems (LMS), e-Learning has become a defining characteristic of this technology adoption in academia (Assefa, 2009). Along with the high intake of this technology are questions of access, usability, and ultimately the questions of how the value of e-Learning can be maximized in order to achieve educational objectives in a modern university.

As an e-Learning tool, the LMS operates as a web-based medium that delivers the essential functionality instead of just serving as distance or electronic learning mediums or places to post the class syllabus (Scalise, 2004). A typical LMS contains the content building and linking tools, as well as tools to facilitate the construction of learning by participants in an electronic course. Such tools include threaded discussion forums, online assignments, problem-based learning tools, tools to facilitate group work, and a variety of real time communications tools (Beebe, 2006).

The increased adoption of teaching and learning technologies in academia is paralleled with a belief that the LMS will enhance teaching and learning processes in academia. Institutional and policy statements for example, assert that one of the core roles of a higher education institution as being to "provide effective advancement of all forms of knowledge and scholarships" (Mlitwa, 2005b, in Erwin et al, CIRN2005: 187-188). This sentiment is accepted by academic and government institutions in many parts of the world. In South Korea according to Jung (2000), the government revised the Lifelong Education Law (1999) that indicates a commitment at university and state levels, to improve processes and means of teaching and learning. In effect, massive resources are invested in research that seeks to find better teaching methods, pedagogy, and to understand learning styles and enabling tools. From these research initiatives, the use of Information and Communication Technology (ICT) such as multimedia, computers, and Internet-enabled tools in teaching and learning have grown in prominence within the functions of a modern university.

As an educator, the researcher is curious about the value that e-Learning technology adds to teaching processes. Equally important is the understanding of the security of content (against unauthorized amendment or even removal of content, tests, and marks) as well as access to and

usage of e-Learning platform. Understanding the security aspect of e-Learning however, requires clarification of the phenomenon of e-Learning, and its uses in enabling teaching and learning processes in academia. The clarification of concepts is outlined on section 1.1, followed by the phenomenon of e-Learning is discussed in detail under the e-Learning innovation section, section 1.2.

The rest of the chapter is structured as follows: The background to the research problem is presented in section 1.3 and the research problem in subsection 1.3.1, followed by the research objectives and the rational in sections 1.4 and 1.5 respectively. The research question is presented in section 1.6. The conclusion is outlined in section 1.7 (which includes the outline of the rest of the thesis in sub section 1.7.1) delimitation of the study on section 1.8, and the chapter closes with the contribution of the study.

1.1 Clarification of Concepts

Whilst all terms are defined as they are applied in the body of the thesis, key concepts of the study are defined in the following section.

1.1.1 Definition of Key Terms

e-Learning	Refers to a technology based learning in which learning materials are delivered electronically to remote learners via computer networks. It may cover a wide set of applications, systems and processes such as e-Learning systems, web-based learning (Assefa, 2009)
LMS User Awareness	Refers to user's knowledge and understanding about the LMS; what they use it for, and application programs used to enhance teaching and learning.
Security Awareness	Refers to user's knowledge about guiding security policies, rules and procedures. Officials who are responsible for providing and administering networking services in a university understand the significance of security aspects. The level of awareness is indicated by their (1) familiarity with key security aspect when working on networked systems, (2) statements that suggest security to be high priority in internetworked systems, and lastly, by (3) adequacy of security trainings, workshops, policies, guiding rules, procedures and compliance system.
Security Threats	Refers to hindrances that leave the networked systems open and vulnerable to threats. These include viruses, pop-up messages, denial of service, lengthy response time, and user challenges about the use of the LMS.
Security Measures and their implementation	Refers to precautions that are practically taken to avert risks to the safety of information stored and exchanged over a networked LMS, that are posed by the system's interconnection to the worldwide web (www). The extent of security measures implementation to protect the network and the LMS against unauthorized access, viruses, denial of service, disruptive interruptions, inappropriate software,
IT/Network Administration	This refers to the department responsible for the computer and network services at CPUT. The department is now called Computer and telecommunication services (CTS) department which was formed after the merger of Peninsula and Cape Technikons in 2005.

1.2 The e-Learning Innovation

E-Learning according to Hassler (2001) refers to a form of learning using a networked electronic medium where the instructor and student are separated by space or time. In this case the gap between the two is bridged through the use of Internet-based technologies. A distinguishing criterion between e-Learning and other forms of ICT according to this definition is that e-Learning should have an internet, network, website or online linkage (Nasseh, 1997; Ingraham et al., 2003). This, in turn, should facilitate the delivery of a learning, training or education program by electronic means across time and distance between the educator and learner (Assefa, 2009; Keats, 2003).

This criterion further gives e-Learning the edge over traditional methods in terms of enabling flexible learning with interactions between teachers, learners, in an online environment, (Czerniewicz, 2008; Georgette, 1997). When unscrupulously interpreted however, flexibility enabling interactions across time and distance may easily result in e-Learning being reduced into a mere distance learning facilitation tool (Mlitwa, 2011). As Ingraham et al., (2003) clearly states, e-Learning covers a wide range of instructional material that can be delivered over a local area network (LAN), or the wide area network (WAN), to provide the learner with information that can be accessed in a setting that is free from time and place constraints, at his or her own pace.

The purpose is usually to enhance knowledge and performance, ideally by offering learners control over content, learning sequence, pace of learning, time, and often media, allowing them to tailor their experiences to meet their personal learning objectives (Bennet & Bennet, 2008; Caeiro et al., 2002). Intranet, Internet, extranet, TV, cell phones and electronic personal organizers (Mlitwa, 2010) are networked technologies that can offer these learning advantages for a student constitute an e-Learning environment. It is clear therefore, that it is the teaching and learning capabilities of an electronic medium, and not whether a student is a distant or face-to-face learner, that describes an e-Learning platform.

Following a discussion on the meaning of LMSs in e-Learning in general, the uses of an LMS are summarized in a tabular format in Table 1. In this table, general agreements in the literature about the features of an LMS are reflected (Mlitwa, 2011). For example, an LMS needs to have a certain minimum capabilities if it is to offer an added value to the tradition non-technology assisted formats of teaching and learning. The five key capabilities that highlight the advantages

of an LMS in teaching and learning processes therefore are introduced and explained in Table 1. The first point is that an LMS should facilitate easy access to learning materials such as notes, lecturer presentations, and other text, audio, video, photographic materials, speedily and conveniently (Table 1). The convenience aspect is in the fact that students can access all facilities from a single point, and at any time. Learning management systems however, come in many designs and formats. The emphasis in this discussion is that for an LMS to offer these capabilities, it should be connected to a network (inter and intranet) that will link users to the content, which has a capacity bandwidth that is sufficient to handle data in different formats, its storage and exchanges.

The connection to the system should also have no time constraints, if the student is to have access it at any time. The speed aspect calls for the network to be protected against unauthorized intrusion by hackers, viruses, and bandwidth consuming spam messages that could divert the attention of the learner, and slow the system. For an LMS to offer fast and convenient access to learning materials for students there should always be at least four things – these are the Internet connection, adequate bandwidth, various aspects of the learning content, and a range of network security aspects. This capability offers a combination of advantages to the learning experience of the student, by providing accessibility (A), efficiency (E), flexibility (F), and security (S) (see the last column of Table 1).

Table 1 further suggests that an ideal LMS should facilitate flexible communication and interaction between students or groups of students, and between students and educators, across time and space. Flexible communication refers to the ability to communicate to someone or to a group of people, both synchronously and asynchronously, regardless of where parties are located. Another aspect of flexibility is the ability to use various formats of communication as may be preferred at any point. For example, communication should be possible in many ways: audio, in text (through written messages), through exchange of written documents, the use of video, and even by using pictures, and all these should be available by navigating between various features in one system and without having to change venue.

Table 1: A Literature Based Description of an Ideal LMS

Key Capabilities	Benefits/ Value added	For* T, L	Necessary Condition/s	Category** A, E, F, S
Facilitates easy access to learning facilities	Fast, convenient & efficient access to lecture notes, lecture presentations, reading material, and other learning content, at the touch of the button and while sitting at one point.	L	For an LMS to offer these capabilities, it should be connected to the internet, and to all the necessary learning and reference materials – for 24 hours, 7 days a week, 365 days a year. It should also be embedded with safety features to prevent unauthorized intrusions or threaten the normal flow of functionalities.	A, E,F,S
Facilitates flexible communication & interaction across time and space	Enable text, audio and picture information exchanges between one or more parties regardless of time and space. Enables group discussions, online collaborations, and immediate response from lecturers and groups in separated locations.	T, L	LMS should have synchronous & asynchronous communication features to bridge distance & time limitations, and enable group discussions. It should also have picture, text and voice handling facilities to enable different formats of information exchanges. This should be supplemented by adequate bandwidth. Safety features are also important to ensure that communication is limited to authorized parties.	F, S
Simplifies course management	Helps manage learning activities, i.e. load course content & define access rights to content. Helps track & guide progress through text or chat interaction.	T	LMS should have a storage facility that can handle audio, picture, text, and the general electronic multimedia data. For this, adequate bandwidth is needed. Security is essential to control access and to protect content.	A, E, S
Simplifies assessments	Enables online assessments (exams and tests), as well as submission & marking of assignments. Simplifies marks administration.	T, L	LMS need features & software to handle short & long question–type assessments (enable uploading, downloading, marking, and the reporting of test, exams, & assignments). Security to ensure assessment integrity.	A, S
Facilitates flexible learning	Students get more control over learning process, improve learning outcomes and maximizes students engagement	T, L	LMS should be designed with interactive features, and be embedded with flexible pedagogy, without compromising the integrity of the learning content, learning process, and the privileges of registered learners.	E, F, S

Explanatory Notes: * **L** = Learner; **T** = Teacher. ** **A** = Accessibility; **E** = Efficiency; **F** = Flexibility; **S** = Security (Mlitwa, 2011: 35)

Clearly, specific conditions should be met in the design, for an LMS to have these capabilities. When designing an LMS using local resources based on open source software, or when one acquires a proprietary LMS for example, it is important to ascertain whether an LMS has the adequate features and functionalities to enable these capabilities.

1.2.1 System Access Control as a Security Function

To start with, an LMS should be capable of facilitating online assessments such as assignments, tests, and examinations when needed by the educator. Students should be able to submit on the due date, the system should be able to evaluate, and report the marks to the university marks administration department, and to publish marks for students to view. The obvious conditions for this facility to succeed, should be the presence of the software to handle long and short question assessments, as well as related marking capabilities. This facility should not of course, be accessible (A) all students registered in the course, but only to those who are registered, not their genius cousins who graduated with a distinction the previous year, which is a case of access control. Access control is a significant element of network security (S), and it goes along with a need to ensure integrity in the assessment (evaluation) process (Schaefer et al., 2009). An assessment should be as free from cheating as is administratively possible (Savola, 2009), and an LMS based assessment should offer no less security (S). An adequate e-Learning platform clearly needs to be supported by very good security and privacy features (Apampa et al., 2008; Van Niekerk & Solms, 2003) if it is to be trusted by the user.

Finally, a convenient LMS should be capable of facilitating flexible learning. Instead of learning being confined to a classroom environment, flexible learning refers to a student gaining more control over the learning process. Students should be able to continue to view lecture presentation slides, as many times as they want to, long after the formal classroom lecture have finished. Students may send a message to the lecturer when unsure of something, without having to go to the lecturer's office, and they may wake up in the middle of the night and go to the content storage on the LMS to access the study material. Being able to do one's assignment online, and submit it at the same point without traveling to a specific office can save students a lot of time. For the LMS to offer these capabilities however, it should meet certain conditions. It should be designed with interactive communication features. It should be embedded with a flexible pedagogy, and without compromising the integrity of the learning content, learning process, and the privileges of registered learners. So, flexible (F) learning, efficient (E)

communication, and a secure network and learning environments, are the necessary conditions for an LMS to be able to provide flexible learning.

It has been clearly shown in this discussion that five conditions are necessary for an LMS to offer advantages of learning flexibility and convenience for the learner; to enable communication between participants in a teaching and learning environment across time and space and to simplify management of the course by the educator. The following necessary conditions are identified: Accessibility (A), Efficiency in terms of speed and precision (E), Flexibility (F) in terms of enabling multiple tasks over one system, regardless of time and user location, as well as ensuring the safety and security (S) of the platform, the content, and procedures.

The significance of these observed points is evident in the attention they receive in many studies, and in academic (Johansen, 2001) as well as technology related (Rosswall, 1999; Mlitwa, 2005a) conferences held on the subject of e-Learning. Studies by Squires (1999), Feldstein (2002), and Miller (2005) for example, have placed high significance on access and accessibility to ICT. Similarly, studies by Allan (2002); Jeffels (2005), Mlitwa (2011) among others, have argued strongly for flexibility, efficiency, and usability of networked technology and multimedia.

1.2.3 System Flexibility as a Security Function

Secondly, an LMS should have synchronous and asynchronous communication features to bridge distance and time limitations in an interaction (Assefa, 2009). Adequate bandwidth capacity becomes even more important in the case of enabling various content storage or exchanges, for example, audio, video, and pictures in high resolution quality may slow or freeze the system in an intranet, when operating under limited bandwidth circumstances (Mlitwa, 2011). Whilst the speed may also depend on the user's connectivity capacity, it is always better when the problem is not on the university side because this situation gives a student the option to change their work station to a more capacitated one to improve access.

If the problem is on the side of the university, a student would be unable to improve their situation, regardless of the capacity of their own connectivity away from campus. When complete communication flexibility is achieved however, there are still challenges to be considered and overcome: a student needs to be sure that they are communicating with who they intend to be communicating with, when a student exchanges files, they do not want to end up with virus infected files, nor does the course facilitator want to end up communicating with strangers who

are not part of the course. Network security and access control matters, are equally-important as flexibility aspect as well. So, the most critical condition of the flexible communication capacity are the flexibility features (F), and security (S) features in this case.

1.2.3 System Usability as a Security Function

Thirdly, as the title "management system" implies, an LMS should help simplify the management of the course – for the educator. A flexible LMS should have a storage capacity to enable the upload and download of learning facilities (Assefa, 2009). The educator should be able to enroll registered students, monitor, and guide progress in the interactions and learning processes taking place over the system. Adequate bandwidth is crucial in enabling the storage of a variety of contents, in various formats as may be required in the course (ibid). In addition to bandwidth, security aspects become crucial when it comes to a definition and the granting of access rights to the stored content. The two conditions that should be met by an LMS in this case are those of adequate online space or repository capacity, access (A) and security (S) features.

This study investigates the security aspects of e-Learning and learning management systems (LMS) as platforms for teaching, learning, and the handling of assessment processes. A background to the research problem to this effect is discussed in section 1.3.

1.3 Background to the Problem

As reflected in Table 1, e-Learning management systems (LMSs) offer many benefits to both lecturers and learners. For the lecturers, the LMS helps them to manage teaching and learning activities, i.e. to load course content and to define access rights to the content. It assists in the tracking and guiding of progress through text or chat interaction. It also simplify, course management processes such as the setting and marking of assignments, marks administration, managing class lists, controlling student's access to study material, as well as to managing and to controlling various courses and assessments (exams and tests) (Paulins, 2010; Weippl & Ebner, 2008). For an LMS to offer all these capabilities, it should have a storage facility that can handle audio, picture, text, and the electronic multimedia data in general. In order to achieve this, adequate bandwidth is needed and security is essential to control access and to protect content (Hayaati et al., 2010). An LMS need features and the software to handle short and long question–type assessments (enable uploading, downloading, marking, and the reporting of test, exams, & assignments). It also needs security to ensure learner assessment integrity (Apampa & Wills, 2008).

For a learner, the LMS should help them get more control over the learning process, maximize their engagement and ultimately, contributes towards improved learning outcomes (Eom, et al, 2006). It should also provide quick, convenient and efficient access to the lecture notes, presentations, reading and study material, and other learning content, just at the touch of a button and from a single location (Clark & Toto, 2006; Beebe, 2006). An LMS however, needs to be connected to the Internet, and to all the necessary learning and reference materials – for 24 hours, 7 days a week, 365 days a year for its potential to be fully realized. It should also be embedded with safety and security features to prevent unauthorized intrusions that threaten the normal flow of functionalities (Apampa et al., 2008).

For lecturers and learners, an LMS should also enable group discussions, online collaborations, and immediate response from lecturers and groups in separated locations (Jeffels 2005; Allan, 2002). LMS should have synchronous and asynchronous communication features to bridge distance and time limitations, and enable group discussions (Lokken, 2011). This should be supplemented by adequate bandwidth Table 1. An LMS should be designed with interactive features, without compromising the integrity of the learning content, learning process, and the privileges of registered learners.

On an e-Learning system, assessments need to be in an environment that is at least as secure as it would be in a paper based test (Apampa et al, 2008). With a paper based test, the students use their hand writing on single versions or copies of assessments and assignments, in the presence of invigilators who can check and enforce integrity (Lorenzetti, 2011). In a paper based system, there are minimum chances of mark change or system errors because marks are allocated manually and put on each assessment copy for report purposes. The marks that are written on each copy cannot be changed without due authorization of an educator. On a computer system, there is a possibility of marks being altered or deleted with or without a trace of intrusion (RT_IT, 2009). There is a need to secure the tracking of marks and submissions of assignments within the marks administration systems in universities.

The current marks tracking system, System for Award Management (SAM) 2007, used at CPUT often lacks consistency in recording different versions of assessments (ibid). For example, students have three chances of submitting assignments. If they get a low mark on the first attempt, they are given second and third chances to improve their marks. Instead of showing the correct mark for each attempt, the system substitutes the first attempt mark with a zero regardless of the mark a student obtains in subsequent attempts. Although a correct mark is

recorded on the educators report, the student gets an incorrect version that shows a zero - which gives a misleadingly untrue record to the student (ibid.).

For assessments in general, online test visibility needs to be secured by randomizing or scrambling tests questions. That is, if several students are writing a test at the same time, their test questions must be different from each other's. For example question one for each student needs to be different from the question one of any of the other students (Van Niekerk & Solms, 2003). All the test questions need to be randomized. In order to ensure integrity of the assessment, the system has to only accept the first submission of the online test. To minimize chances of assessment manipulation and abuse, the system should block any unauthorized re-submissions of the same assessment (Marais & Argles, 2006).

According to the literature, five conditions are necessary for an LMS to offer advantages of learning flexibility and convenience for the learner (Mlitwa, 2011). The same conditions are also necessary to enable communication between participants in a teaching and learning environment across time and space, and simplified management of the course by the educator (Dietinger, 2003). The following conditions are identified as necessary: Accessibility (A), Efficiency in terms of speed and precision (E), Flexibility (F) in terms of enabling multiple tasks over one system, and no matter where the user is located, as well as the safety and security (S) of the platform, the content, and procedures.

The significance is clear in the attention these conditions receive in many studies, in academic (Johansen, 2001; Jerz, 2003) as well as technology related (Rosswall, 1999; Mlitwa, 2005a) conferences held on the subject of e-Learning. Studies by Squires (1999), Feldstein (2002), and Miller (2005) for example, have placed high significance on access and accessibility to ICT. Similarly, studies by Jeffels (2005), and Allan (2002), among others, have argued strongly for flexibility, efficiency, and usability of networked technology and multimedia. The security (S) aspect however, overlaps across all these criteria. Effective and flexible access for example, depends on how safe the network is, and whether rights to content access have adequately been defined and effectively controlled (Mlitwa & Birch, 2008). Similarly, flexibility can be threatened by unauthorized access, and also, by uncontrolled spamming, unwelcome viruses and worms (Alwi & Ip-Shing, 2010; Marais & Argles, 2006; Kabay, 2006). Efficient management of the course and assessments both depend on the same criteria (Gillespie, 2012). Whilst the A,E,F criteria for the use of an LMS have received a significant attention in the literature, the same cannot be said of the security (S) aspect (Weippl & Ebner, 2008). However, the fact that

security overlaps in all the other criteria suggests that security should hold a higher level of significance when judging the usefulness of an LMS for teaching and learning.

The benefits of using LMSs in teaching and learning processes however, are not fully exploited by educators in most departments, and in particular, the Department of Information technology at CPUT, for a number of reasons, one of which, security limitation stands out. The effects of security limitations are discussed in section 1.3.1.

1.3.1 Security Limitations

Most of the researcher's colleagues in the department of Information Technology, in a conversation on 27 March 2009 Mak_IT and 25 March 2009 Tmak_IT for example, do not use all the functions of Blackboard. They only use Blackboard for assignments, announcements and the posting of the course material. They cite network trust-related problems as an inhibiting factor to the full use of the current LMS in the institution. In a conversation on 27 March 2009 Mak_IT stated that his students for example, uploaded the programs into the system, but the program got lost before being captured. While, he was downloading the class list, he had to access more than six files in order to locate a single student on the class list. Similarly,

In a conversation on 23 March 2009 Rx_IT and Fe_IT stated that they are only using the LMS for assessments, course material, assignments and announcements. They cite as a security hindrance the failure of the LMS program to disable other windows when students are taking assessments. For example when students are writing a test, it is possible for them to minimize the test window and refer to the course material from their H drives, internet and other lecturer's material. Rx_IT further gives an example where one student retrieved a solution from the online notes, changed the font and submitted the solution as his test output in s new format. This one student copied almost all the answers from the internet and ended up pasting the information from another sources into his test. In order to secure online tests, the page or the test window must remain opened and locked until the student finishes and submits the test. Only after the test has been submitted should the student's window be enabled to browse other windows.

The lack of this basic level of security on the CPUT LMS platform, remains a hindrance to full usage of the system by lecturers in the IT department, if not the whole institution. As an educator with similar frustrations, the researcher decided to undertake an investigation into the security aspects of the e-Learning system used at CPUT, with particular reference to security of the course content, assignments, assessments processes, submitted marks and class lists. E-

learning security is essential if e-Learning is to be established as a trusted support or a primary education platform for learners and as a routine course management system for educators. In order to prevent unauthorized access to sensitive or even privileged content, and to limited hindrances access, it is necessary to consider techniques that would improve the security of the LMS as well as to limit distortions and disruptions to online learning, teaching and assessment processes. It is for this reason, that the security component of an LMS in an e-Learning process is selected for investigation in this study. The research problem is set out in detail in section 1.3.2.

1.3.2 The Research Problem

An ideal LMS needs to offer benefits to both student and educators (see Table 1). It has to simplify and improve teaching and learning processes. Now, given the significance of security considerations in all the aspects of an LMS, it is clear that security should form a significant part of all LMSs. As an educator in a progressively more challenging environment, with many classes and various groups of learners, the researcher recognized the importance of the use of e-Learning technologies such as LMSs and the advantages they promise to teaching processes. Whilst the university has made an e-Learning platform available for educators to use and benefit from its advantages, it has not been possible for the researcher and her colleagues to exploit the full benefits of this technology. The researcher's department that is part of the Faculty of Informatics and Design (FID) is exploring the use of e-Learning for assessments, teaching and learning.

Researcher's observations in the IT department are that a number of educators are not even aware of the benefits that e-Learning may bring to their teaching tasks. The minority that keeps exploring its uses are discouraged by lack of consistency and usability. The result is that many of them are not making any use of the e-Learning facilities at all, even though a few lecturers do use the LMS for assessments.

Currently the researcher is using the departmental LMS known as Blackboard for the submission of marks, tracking of marks, class lists and assessment. The problem that has been encountered with marks is that, the system sometimes does not show how many marks the student obtained on that specific test, until the second chance is granted to the student. The system does not change its report as it should, if the time has expired or if a student resubmits within the given time. That means, marks or attempted questions can only be seen on the system when the

student re-attempts the test and the test will continue where it stopped before the cut off. The test will show what questions have been attempted and what questions have not been attempted. The cut off time of the test can be caused by unforeseen circumstances, such as a power cut, viruses, and insufficient bandwidth to accommodate class groups or university network congestion among others. It would be helpful if the system could at least show simultaneously to the lecturers when an assessment is not completed.

One problem that student's experience when doing assessments is frequent disruptive cut-offs whilst in the middle of online exercises. Another major problem is experienced with security. The windows, which should not be flexible enough to be minimized when the students are busy with assessments, are easily manipulated by learners during assessments. If the assessment window can be minimized, then that gives learners some time to look for the answers elsewhere. They can search on the internet and on their local drives (such as the H: drive at CPUT) where all students registered in a course can access the course content or even access their own memory sticks. Sometimes the pictures on the assessments cannot be seen clearly by the students and at other times they cannot be seen at all.

What has come to light is that in the IT department there is a lack of understanding not only of e-Learning systems but also of the concerns on how safe it is to use for assessments. Lack of security, or even perceptions of limited security, in a networked platform, in an area such as e-commerce (Mjuleni & Mlitwa, 2008) or an e-Learning environment (Mlitwa, 2010) it is argued, limit interest in and usage of that a technology. While use is limited no-one needs to make any efforts to address the security issues, as a result, the negative perceptions remain, and usage remains limited. When usage remains limited, learners do not benefit from the advantages they would otherwise derive from maximum usage of LMSs in higher education (HE).

In trying to understand the problems faced by e-Learning from the literature, it regrettable that despite the acknowledged importance of security in almost all aspects of e-Learning, very little attention has been paid to the security aspect of e-Learning and its LMS tool in current research (Weippl & Ebner, 2008). Neither is it clear whether or not the security issue is receiving attention in any current e-Learning initiatives at CPUT as an institution. It is also unclear in the existing literature what if any level of awareness of the security issue exists, in the e-Learning departments that plan and administer LMSs, or in the IT support departments, or within the academic staff that implement e-Learning. In addition, the level at which security aspects of e-Learning are discussed and implemented within e-Learning departments, within IT support

departments, and at all academic levels, not only at CPUT but at other South African universities, is also unclear.

The significance of the security aspect in e-Learning suggests that it should be prioritized, first, at the design stages of the system, and secondly, at all layers of the implementation process. When security issues have been discussed and clarified, it will be necessary to check how to fully exploit LMS benefits for CPUT e-Learning.

Having outlined the uses of e-Learning tools in teaching and learning, the objectives of this study are discussed in section 1.4

1.4 Research Objectives

For maximum benefits to be derived from e-Learning practices, it is important that it is prioritized at decision making, at academic planning, at technology and network support, at educator, and at individual learner levels. For this to happen it is necessary, in the first instance, that planners, implementers, and users are at least aware of the significance of adequate security in e-Learning in terms of assessments, content, class lists etc. The significance of security is broadly discussed in the background to this study. Therefore, the objective of this study is to understand the extent to which security measures associated with e-Learning practices are implemented at e-Learning administration, at IT network administration, at academic planning, and at the educator levels. This involves understanding of the level of e-Learning related security awareness that exists within e-Learning administration structures, with IT network administrators, in academic planning departments, and with academics that use e-Learning facilities at universities. Understanding the status of existing tools, rules and practices is also a significant part of this investigation. The goal of this study is to bring insights about the level of security awareness among LMS users, the usage of the security measures in higher education institutions as well as informing suggestions about adequate usage of security measures to mitigate threats on the LMS. The rationale for the study is outlined in section 1.5.

1.5 Rationale

Many universities are either at an early stage of some e-Learning adoption or have fully implemented one or more aspects of it – in supporting the teaching and learning (Gunasekaran et al., 2002). The University of the Western Cape (UWC), University of Ghana, and the Kabul Polytechnic University (KPU) in Afghanistan, among others, has completely moved to the

Knowledge Environment for Web-based Learning (KEWL) as their e-Learning platform (UWC, online; Angel, online). KEWL is an Open Source product that is available free to anyone who wishes to use it for educational, commercial or any other purpose (Beebe, 2006). Another example is the University of Cape Town, which uses an open-source learning, collaboration and research content management system known as VULA (UCT, online). Similarly, the Cape Peninsula University of Technology (CPUT) and Stellenbosch University (US) are using a proprietary learning management system known as Blackboard (CPUT, online; Stellenbosch, online) as an e-Learning platform.

As an educational platform that simplifies and improves teaching functions such as the tracking and submission of marks, managing assessments, managing class lists, controlling student's access to study material, as well as to managing and controlling various classes and courses, e-Learning technologies may be vulnerable to distortion errors, or even manipulation and abuse.

Since the university has made an e-Learning environment in the form of a Blackboard LMS platform, being able to fully exploit its capabilities may enable an educator to maximize the benefits that can be obtained from e-Learning. Members of the IT department within the Faculty of Informatics and Design (FID) are exploring the use of e-Learning for teaching, learning, conduct assessments, and for marks handling and reporting. With regard to assessments, initial observations highlight that the security of the course content, test, assignments, submitted marks and class lists against unauthorized access and manipulation are in need of urgent attention.

The research question is outlined on section 1.6.

1.6 Research Questions

The objective of this study is to understand the extent to which security measures on e-Learning practices are implemented at e-Learning administration, at IT network administration, at academic planning, and at the educator levels. This involves acquiring an understanding of the level of e-Learning related security awareness that academics and students have, who use e-Learning systems. However, the main research question is: What is the status quo of the security aspect in e-Learning systems at CPUT, Western Cape, in South Africa. To find answers to the questions, a method of enquiry is selected and discussed. This is done in chapter three of this thesis.

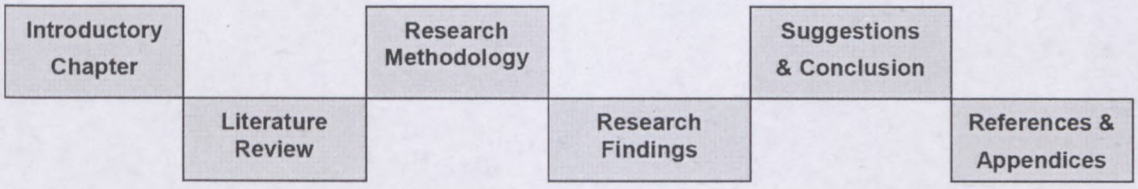
Table 2: Research Question

Research Question: What is the status quo of the security aspect in e-Learning systems at CPUT, Western Cape, in South Africa.			
Sub research questions			
How is the level of LMS awareness by e-Learning users	**What are the current security related awareness programs**	**What are the existing security threats**	**What are the existing security measures and their extent of implementation**
Sub questions: • What do students and academics use LMS for? • Do you use instant chats and discussion features • Do you find it easy to work with the LMS? • How is the login details generated? • What are the criteria for one to get access rights to a course? • How are access controls such as passwords, and usernames, made effective? • What type of data formats does the LMS handle? • What data handling programs do you have in place?	**Sub questions:** • Were you trained to use the LMS? • Who facilitated the training? • Rate your level of understanding? • Do you know of any guiding security policies in place? • Have you been introduced to any LMS security usage? • Are there any policies that are in place regarding users with unauthorized access? • If there are, how are they communicated to users? • Have you signed the security compliance form? • And how often do those compliance programs run? • Are there people who breach security policies? • Are the e-Learning users all computer literate?	**Sub questions:** • What security threats do you encounter? • How often do users encounter those threats? • How do users handle those threats? • Do academics encounter any problems relating to the LMS usage? • What types of computer and network problems do you encounter? • Do you encounter any hindrances such as viruses, pop-up messages, and denial of service? • To whom do you report those challenges to? • How long do challenges take to be fixed? • What challenges do academics have relating to LMS online assessments/ • Do academics encounter students with unauthorized access?	**Sub questions:** • How do academics protect critical information on the system? • How long are the LMS passwords and their combination? • How long does it take for the login details to expire? • What security measures do you think should be implemented to protect critical information? • Which security measures used against viruses, denial of service and pop-up messages? • Are they always up to date? • How often do they update them? • Who is responsible to update the system? • How are spam, denial of services and pop up messages prevented? • What are the current security measures for user access to the system? • How do you prevent a lengthy response time? • Is there enough bandwidth, and hardware space to accommodate the learning material?

1.7 Chapter Conclusion

This chapter begins by introducing the background to the research. The chapter goes on to discuss e-Learning innovation, background to the research problem, the research objectives, the rationale, and the research questions. There is clarification of the terms used in this research, as well as a delineation of the current research. The chapter closes with the contribution that this research is expected to provide to the beneficiaries.

1.7.1 Thesis Structure



This dissertation is composed of seven chapters that are outlined as follows.

Chapter One Explains the background, the research problem, and the aim of the study.

Chapter Two Reviews the literature for the study by discussing background to e-Learning systems in Higher Institutions. Uses an Activity Theory as a lens to understand the security aspect of e-Learning system.

Chapter Three Presents the research design and methodology used in this study.

Chapter Four Analyses data collected from the information gained from questionnaires, interviews conducted with CPUT academics, students from IT department as well as the network administrator. This chapters further discusses the findings of the research.

Chapter Five Outlines the achievement of the aims of study and concludes with recommendations for future research. The thesis closes with the list of references and appendices attached.

1.8 Delineation of the Research

The objective of the study is to achieve three things. Firstly, to understand the level of e-Learning security awareness, secondly, to understand the extent to which security measures on e-Learning are implemented at higher education institutions and lastly, to explain the emerging patterns. This enquiry is possible only if the meaning of security awareness is clarified. Similarly, security measures of e-Learning, as well as the meaning of implementation should be clarified.

The e-Learning administration structure, the IT network administration, and academic planning departments also need to be clearly articulated.

The contribution that is expected this study is outlined on section 1.9.

1.9 Contribution of the Research

The objective of this study was to understand the extent to which security measures on e-Learning practices are implemented at e-Learning administration, at IT network administration, at academic planning, and at the educator levels. This involved the understanding of the level of e-Learning related security awareness by academics and students that use e-Learning systems.

Despite these conditions: Accessibility (A), Efficiency (E), Flexibility (F) and Security (S). It is the security aspect that clearly spreads across all criteria in the discussion. Effective and flexible access for example, depends on how safe the network is, and whether rights to content access have been adequately defined and effectively controlled. Similarly, flexibility is threatened by unauthorized access, and even more so, by uncontrolled spamming, unwelcome viruses and worms (Kabay, 2006). In addition, the fact that security is so important for the achievement of all the other criteria suggests that it should occupy a very high level of significance when the usefulness of an LMS for teaching and learning is being considered. It is for this reason, that the security condition of an LMS in an e-Learning process is selected for investigation in this study.

Therefore, it is hoped that the study will benefit the university at large by providing useful insights into at present unknown or poorly understood levels of e-Learning. This is to be achieved by looking at and understanding the current levels of e-Learning related security awareness that exist among users and the current security measures that are implemented. The study will also benefit the research community, e-Learning administration structures, IT network administrators, academic planning departments, and e-Learning users on how to fully use and exploit the LMS benefits.

The Literature study is presented in chapter two.

CHAPTER TWO: LITERATURE REVIEW

2. Introduction

The previous chapter discussed the problem statement; objectives of the study; background to e-Learning systems; key capabilities for an ideal LMS and value added services for both students and teachers. The main research question was posed to address a research problem of this study. This chapter presents a synopsis of e-Learning, with emphasis on the learning management systems (LMS) as an e-Learning tool and, ultimately, the significance of the security component on e-Learning processes in higher education (HE) spaces.

The chapter opens with a contextual background of the phenomenon of e-Learning, including an introduction of this concept, with emphasis on the historical context and local uses of LMSs in higher education. The purpose and value of an LMS in educational processes, together with the components of this tool, are further elaborated in this chapter. A graphical illustration of an ideal LMS is presented in section 2.2 in Figure 1 in this respect. Best practices on the LMS adoption and usage in higher education spaces, with inferences on security and usability aspects as well as an outline of security-related challenges to the use of LMSs in modern universities, are also clarified.

An Activity Theory (AT) is then used as to contextualise an ideal security environment for an LMS in higher education spaces.

2.1 The Context of e-Learning in HE Spaces in South Africa

Various researchers understand and interpret the e-Learning term in a number of ways. For example, Govindasamy (2002) and Assefa (2009) describe e-Learning as a fundamental way of teaching and learning, where an instruction is delivered via the electronic media such as "Internet, intranets, extranets, satellite broadcasts, audio/video tape, interactive TV, and CD-ROM". In this context, e-Learning is presented as a useful process where teaching and learning is mediated by interactive (and non-interactive) technologies. With respect to interactive technologies, networked technologies provide interactive capabilities between the teaching and learning parties (ibid). In this case, an internet-based Learning Management System (LMS) is able to facilitate open, flexible and distributed learning beyond the confines of distance, time and space (Hotrum, 2005).

In the case of non-interactive technologies on the other hand, the audio/ video tape and a CD-ROM are electronic devices that contain uni-directional and pre-recorded type of information, where the learner can only listen or read, without any form of interactive discussion. This means

that teachers and students could engage on a constructive discussion and can get an immediate response about any question posed. Clearly, the common denominator between non-interactive and interactive technologies is the aim to enhance teaching and learning over an electronic interface.

In a different account, Carliner (2005) and Czerniewicz et al. (2006) explain e-Learning as the deliverance of study material to learners through the use of the Web. In this context, there is no face to face contact with the learners or actual hard copies of study material that are given to students. The implication in this case is that of direct instruction and storage, where a networked interface is used as tool to distribute educational content. On the other hand, Mlitwa (2006) emphasizes the centrality of Web-enabled platforms in e-Learning. Mlitwa describes e-Learning as the use of different technological tools that can either be web-based or web capable, for the purposes of facilitating education, where the "hardware and software environment for network-enabled learning programs and processes" becomes the critical components.

Whilst these definitions are somehow different contextually, they all emphasize the use of some form of an electronic tool, platform, medium, or tool as a teaching and learning interface, across pedagogical domains (Mlitwa, 2011). Similarly, the motive of a LMS as an interactive tool, platform or interface of e-Learning, is to facilitate learning over a virtual platform (Arth, 2011). As used in this study, e-Learning is understood as the use of Web-enabled technology platforms to facilitate learning across distance, time and space. In this case, teaching and learning activities takes place through a shared medium – LMS, where students access the learning material posted by the teacher on an LMS. The concept of e-Learning can be further described in terms of its key purposes and benefits to stakeholders.

2.1.1 Benefits of e-Learning to Educational Processes

E-Learning systems provide a number of reasons to universities including enhancing teaching and learning; and ultimately provide quality learning to students (Mlitwa, 2011). In essence, e-Learning is implemented through the use of the LMS tools to deliver learning through the networked systems (Brennan & Shah, 2003). One of its primary activities achieved through the use of LMS and other available tools in a shared administrative interface where electronic online courses are assembled and used (Nichols, 2003). As reflected in Table 1 (in chapter one), e-Learning systems should improve efficiency, flexibility by providing adequate access to resources and learning material in a form of graphics, sound, animation, and multimedia (Assefa, 2009). They should further provide students with control over learning at their convenience. In this context, students should be able to access the learning material anywhere and at any time of the day. In addition, an e-Learning system should support communication between the teacher and

students and between students, with synchronous or frequent asynchronous feedback (Carliner, 2005). This means that teachers should at the very least, be able to communicate with each other and with students on an e-Learning platform. These benefits and purposes have drawn attention to tertiary institutions, with universities in the Western Cape Province having adopted various e-Learning systems to improve teaching and learning activities. In these efforts, Laurillard (2008) sees learning outcomes on e-Learning systems as a major priority, to the extent of arguing that the use educational technology should be founded on a thorough articulation of "what it means to learn" (Mlitwa, 2011). An LMS therefore, should be logically structured to effectively facilitate learner-focused educational processes.

2.2 A Logical Structure of an LMS

If enhancing the quality of learning is the focus of e-Learning practices, then the actual tool should be embedded with enabling components towards this end.

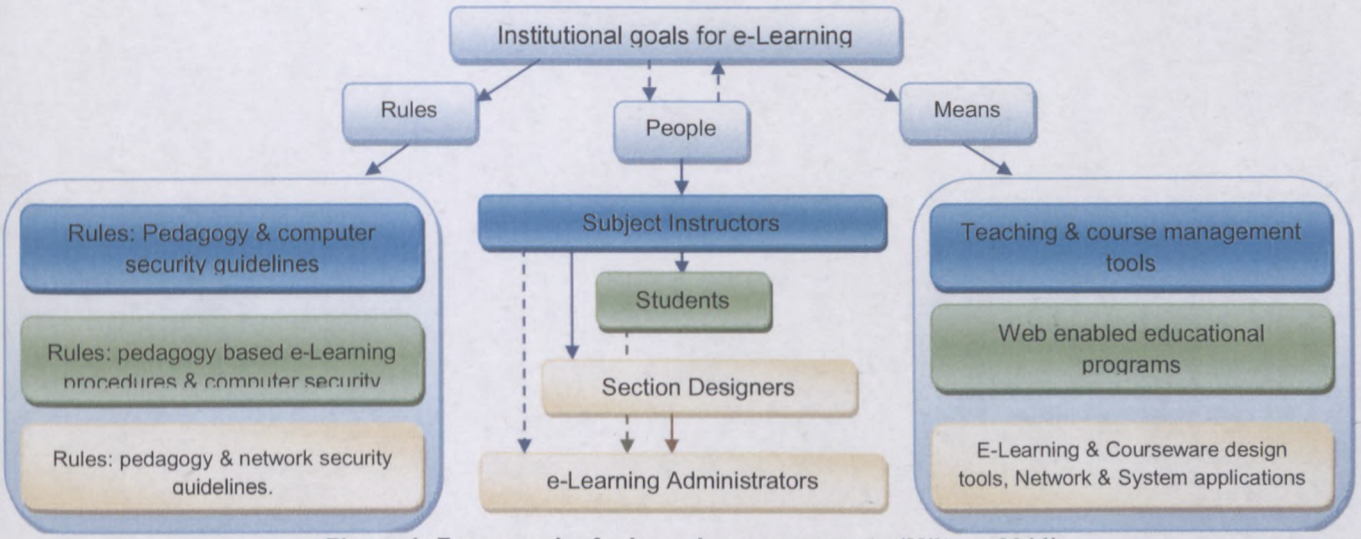


Figure 1: Framework of e-Learning components (Mlitwa, 2011)

Figure 1 outlines four core components of an ideal LMS, which include institutional goals, people that set and pursue the goals, the rules that must be followed and the means of achieving these educational goals.

According to the graphical illustration of Figure 1, the LMS platform should be based on, and reflect institutional goals of teaching and learning. With a direct arrow line (information flow) between the goals and people, it is clear that institutional goals do not stand alone but are embedded in stakeholder roles and responsibilities. These goals reflect beliefs as translated into roles and responsibilities of the stakeholders (subject instructors, students, section designers and

administrators) in the e-Learning environment. The same goals are translated into rules of which, pedagogy, computer security policies and network functionality guidelines are key to the purpose of this study. Obviously, goals and policies mean very little if not translated into e-Learning related activities, which calls for their coordination with relevant process enablers. These refer to e-Learning tools such as the teaching and course management tools, web-enabled educational tools as well as courseware design, network and systems application tools.

In fact, the activity theory is used to contextualize the security environment of e-Learning to elaborate on this logic in section 2.3. In this section, the theory is used to present the security framework of e-Learning as a coherent and holistic work activity system made of different components that are linked together to form a coherent whole.

2.3 Theoretical Perspective of e-Learning Systems

A theory is a set of organized perceptions explaining interrelation between ideas to illustrate concepts and their relation to each other (Roos, 2012). Friedman (2003) defines a theory as a "... illustration describing how something works by showing its elements in relationship to one another". Use of appropriate theories in research helps to understand and analyze a complex research problem (Charmaz, 2006).

As the study entails socio-technical information systems elements (information, technology, system, communication, organization, and people), a theory has also been used as a lens to understand the transformation process within these interrelated e-Learning systems components and how various user levels interact to achieve the process on transformation in an activity system. Lastly, the theory reflects the theoretical assumptions to carry out the methodology which carries out techniques of enquiry presented in chapter four. However, the current study has adopted an Activity Theory (AT) as a lens to better understand the security aspect on an e-Learning system at CPUT. Assumptions in an activity theory are formed and rooted in its keys concepts. For example, drawing primarily from Hardman (2005, p2), an AT was formulated by Engestrom (1987) including basic principles and assumption of the phenomena such as subjects, objects, tools, community, and division of labor as well as rules (Mursu, et al. 2007). Whilst individuals or groups represent subjects of an activity system, object the common goal (sought objective) in the activity system (Buchem et al., 2011).

At the same instance, mediators refer to enabling factors without which, a transformation of goals into activities and ultimately, outcomes, may not succeed (Carr & Czerniewicz, 2007). Community refers to participants sharing the same object, and the division of roles among members represents a division of labor which in turn informs various activities by respective

actors in an activity system (Buchem et al., 2011). These actors, goals, activities, actors, mediators, transformation and outcome concepts within the activity system are connected together, by a drive towards a common object – the realization of secure an efficient e-Learning environment in a higher education institution such as CPUT.

2.3.1 Activity Theory (AT)

Activity theory (AT) is constructed on Vygotsky's (1978) concept of mediated action in a model, which encouraged duality of the individual and their social environment by associating human actions with cultural artefacts (Engeström , 1987). An activity was viewed as response formulation that entailed an act of mediation. As suggested by Vygotsky (1978) unit of analysis in the initial phases of the application of AT was on individual activities. Engeström (1987) views the mediation of the elements in an activity system as an important aspect of a human activity. However, it is important to pay attention on the "...the focus of the study of mediation should be on its relationship with other components in an activity system" (Engeström, 1987: 29). 53

The focus of AT is on the interaction between human activity, objects or goals and mediators within the appropriate context (Vygotsky 1987). An activity is seen as a factor that ties the actions to the context, hence an activity is a basic unit of analysis in Activity Theory (Engeström, 1987). Since human actions derive their meaning from the context, "actions without context are meaningless" (Mursu et al., 2007: 6), actions must be viewed within a context (Leont'ev, 1978). Rather than a predicted theory, AT is a descriptive framework which can be considered a concept and a theoretical approach or a viewpoint (Mursu et al., 2007). In most instances AT is used to analyse human activity from a needs-based and goal oriented viewpoint (i.e. people are driven by needs and therefore have specific goals to achieve) (Mlitwa, 2011). Consequently it is used to understand human interaction through mediated tools and artefacts (Hashim & Jones, 2007).

2.3.2 Adoption of Activity Theory (AT)

An activity theory is one of the commonly used information systems (IS) research theories which is the most appropriate theory for the study. As defined on the work of Cole and Engestrom (1993), the theory mostly views phenomena of investigation as an activity system i.e. (teams, organizations, etc.) which comprised of activities by actors who work under common rules, guidelines, contexts and conditions known as mediators, in pursuit of a common goal or objective, through the use of tools or artifacts. Its assumptions are that work takes place within the activity system; work happens for a purpose; and the social, cultural and technical contexts motivate or hinder the activity (Mursu et al., 2007; Allen et al., 2011).

According to Korpela et al. (2002) activity is also mediated by a community, a community may also impose rules that affect activity. Activities consist of goal-directed actions that are conscious and constituents of activity are not fixed; they can dynamically change in order to reach an outcome (Roos, 2012; Allen et al., 2011). It is necessary to produce certain objects (experiences, knowledge, etc). Human activity is mediated by artifacts e.g. (tools used, document etc.). In reality, the cultural and technical mediation of human activity and artifacts are not used in isolation. In this case, the unit of analysis is a motivated activity directed at an object and the subject works as part of the community to achieve the object.

Activity theory has three levels of activity that facilitate the positive functionality of an activity system (Kuutti, 1995). The first level as the activity towards an objective carried out by a community, a result of that may not be conscious social and personal meaning of activity. It usually answers the "Why" question (Korpela et al., 2002). The second level presents the action towards a specific conscious, carried out by an individual or a group possible goals and sub goals, critical goals and usually answers the "What" question. And the last level, addresses the operation structure of activity typically automated and not conscious concrete way of executing an action in accordance with specific conditions surrounding the goal, and helping in and answering the "How" question (Cole & Engestrom, 1993).

In an activity theory, there are underlying principles to conduct IS related studies (ibid). The first principle is to be object-oriented, meaning that a researcher should not be limited to the properties that are considered objective according to natural sciences, but also extend the analysis to socially/culturally defined properties as well. The second principle pertains to a relationship between internal and external activities where, internal activities cannot be analyzed separately from external activities due to their inter-linkage towards the transformation process. Transformation in this theory refers to the change of activities through the use of tools to achieve outcomes (Korpela et al., 2004).

The argument is that internalization process transforms external activities into internal activities. It enables people to interact with reality without manipulating real objects. Instead of manipulating sniffers for security purposes on the network, in the current study, the AT would allow a researcher to interview actors who directly work on the e-Learning systems. This could include mental simulations, imaginations as well as to consider alternative plans. On the other hand, externalization transforms internal activities into external ones, which are necessary when internalized action needs to be repaired. Externalization is also important in the coordination of collaborations between people who require their activities to be performed externally (Kaptelinin, 2005)

Mediation is the last principle which put emphasis on human activity that is mediated by tools (Korpela et al., 2004). In this case, tools are created and transformed during the development of the activity, carrying with them a particular culture and historical connotations from their development (Uden & Kumaresan, 2007). In this study, tools can be computers, software, ideas, methods, internet etc. (ibid).The use of tools is an accumulation and transmission of social knowledge. Tools influence the nature of external behavior and also the mental functioning of individuals (Mursu et al., 2007). Therefore, use of tools in an activity system facilitates an outcome which can either be limiting or enabling (Kutti, 1995).

The AT emphasizes interactions between human activities and consciousness in an environment (Vygotsky, 1978). Social transformation within a social setting and contradictions for reasons of change, transition or development, are major components of this process (Uden & Kumaresan, 2007). In the current study, an example of transformation within the contextual setting of e-Learning would be a process of converting a goal, rules and activities – into outcomes (Mlitwa & Van Belle, 2011). Contradictions would resemble tensions between of different actors, their goals as well as access and use of tools, information and information flows, with an inhibiting effect on activities and outcomes. In the current study for example tensions may be expected through the conflict that exists on the mediating factors. For example, a tension is likely to happen when there are networked computers with adequate bandwidth but with unclear network usage policy indicating procedures and clear guidelines towards the usage. Similarly, networked computers that are not up-to date may cause negative outcome.

On this basis, the AT proved to be the most appropriate lenses upon which the e-Learning security phenomenon could be viewed and analyzed in the current study. Relevance of this theory in the study is elaborated in more detail on the section below.

2.3.3 Application of Activity Theory in the Current Study

As used in this study, an AT provides a broad approach in understanding and viewing phenomena from an activity system. As cited on Korpela et al. (2004) an AT "provides a good starting point for developing a framework". It also gives a broader understanding and view of many aspects that make up an activity system. The framework on **Error! Reference source not found.** illustrates different actors with their activities on an e-Learning system; how tools, enabling and inhibiting factors directly affect teaching and learning processes on the system.

AT helps various actors to interact with the system in different levels ranging from individual to organizational to achieve their desired goals. In effect, the AT has been successfully used for similar purposes in a number of studies. For example, studies by Groves and Dale (2004)

successfully applied AT as a lens to analyze coordinating constructivist and socio-cultural perspectives in mathematics learning. Hardman (2005) also used the AT theory in studying human computer interaction in South Africa. Similarly, Mlitwa (2007) also used AT and Actor-Network Theory as an analytic framework in teaching and learning in Higher Education context. Nonyane (2011) used the AT theory to investigate the usage of ICT skills among disadvantaged communities in the Mpumalaga Province. Lastly, Mlitwa (2011) adoption of the framework for the integration of e-Learning System into Academic Programmes in Modern Universities: A South African Perspective.

In addition to its appropriateness, successful use of the AT in a number of these studies promised a possible success in the current project. Actors varying from individual to institution resemble levels of analysis with specific roles they play in an activity system. In essence, AT assumptions made it possible to use and develop the work-activity framework for e-Learning systems in a security perspective and for the analysis of data in chapter five. The term work activity system means a way of categorizing actors performing actions to achieve a specific goal through the use of enabling mediating factors. On the process, transformation will take place to produce an outcome within the framework.

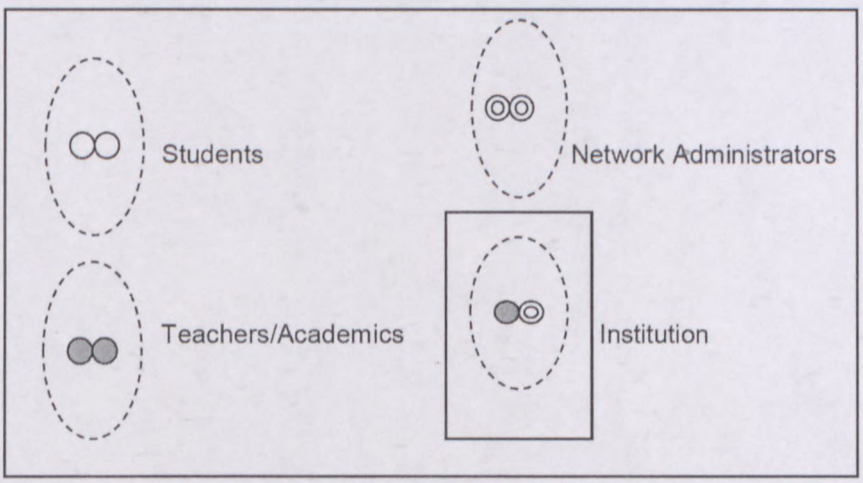


Figure 2: Work- Activity System (Mlitwa, 2011)

Figure 2 presents a work-activity system shortening socio-technical system relating to individual or joint activities facilitated by an LMS as a shared tool. This study addresses four actors varying from one to four which are students, academics, network administrators as well as the institution. Actors assist in developing a work activity framework which is explained below (Mursu et al., 2007). They have specific goals to achieve within work-activity system. Their individual processes are illustrated through the use of arrows to the designated goals.

Students

Students identify units of observations as an individual or group of students playing a major role within the activity system. They use e-Learning System (LMS) to achieve effective learning by easy access to the study material, tests and their marks. The assumption is that student learning content should be able to handle all data formats such as text, voice and picture at the same time. In addition, the shared LMS should provide an instant communication feature for teachers, students and their peers as well as active discussion forums. The LMS should help them access their assessments in a more secured environment. As shown on Figure 3, students perform activities like accessing content; submission of exercises and assignments at their convenience.

Academics

Academics represent the group of academics working together using e-Learning system to facilitate learning within the activity system. As used in the framework, teachers conduct and manage assessments including exercises, assignments and content safely and effectively. They are supposed to facilitate quality learning over LMS in networked computers across the time and space; have control over the learning; to activate test and assignments as well as managing student groups, course content and access to study material.

Network Administrators

Network administrators represent a group of actors responsible for network administration and support of learning through networked computers. Their specific goals are to ensure network security and functionality with 24/7/52 days error free usage; ensuring continuous maintenance by implementing safety measures against threats; scanning of threats and filtering of unauthorized users to provide efficient and effective network to users. However, this can be done through adequate, clear policies; procedures for network usage and implementation. This includes further guide the network users in terms of the security and efficiency.

Institution

Institution operate under the control of management activity representing departments and sub departments responsible for providing proper management and usage of the network; providing direction for implementation of new policies in other departments; responsible for network security management; rules, guidelines and policy formulation as well as setting standards and rules to adhere to when using the CPUT network. **Error! Reference source not found.** presents a Work-Activity Framework for Security Analysis in e-Learning System.

2.4 Activity System

Units of analysis in an activity theory are activity system. Drawing primarily from Hardman (2005, p2), AT was formulated by Engestrom (1997) including basic principles and assumption of the phenomena such as subjects, objects, tools, community, and division of labor as well as rules. A representation of these concepts is shown in a diagram format on Figure 3.

- Individuals or groups represents subject of an activity system
- Raw material that helps to achieve transformation into outcomes represents the objects
- Mediators to achieve positive or negative outcomes denotes tools of the activity system
- Community refers to participants sharing the same object
- Division of tasks and roles among members represents division of labor
- Means that controls the actions are rules

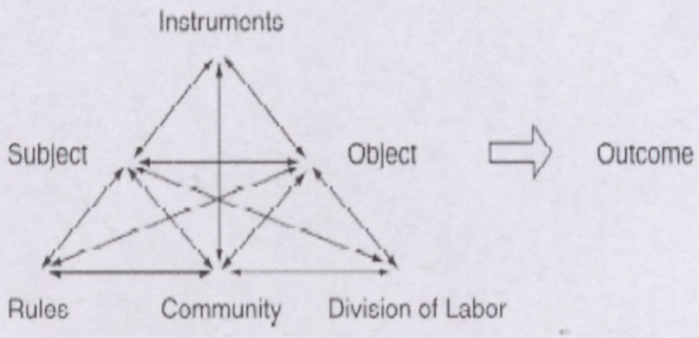


Figure 3: Components of Activity System by Engestrom (1987)

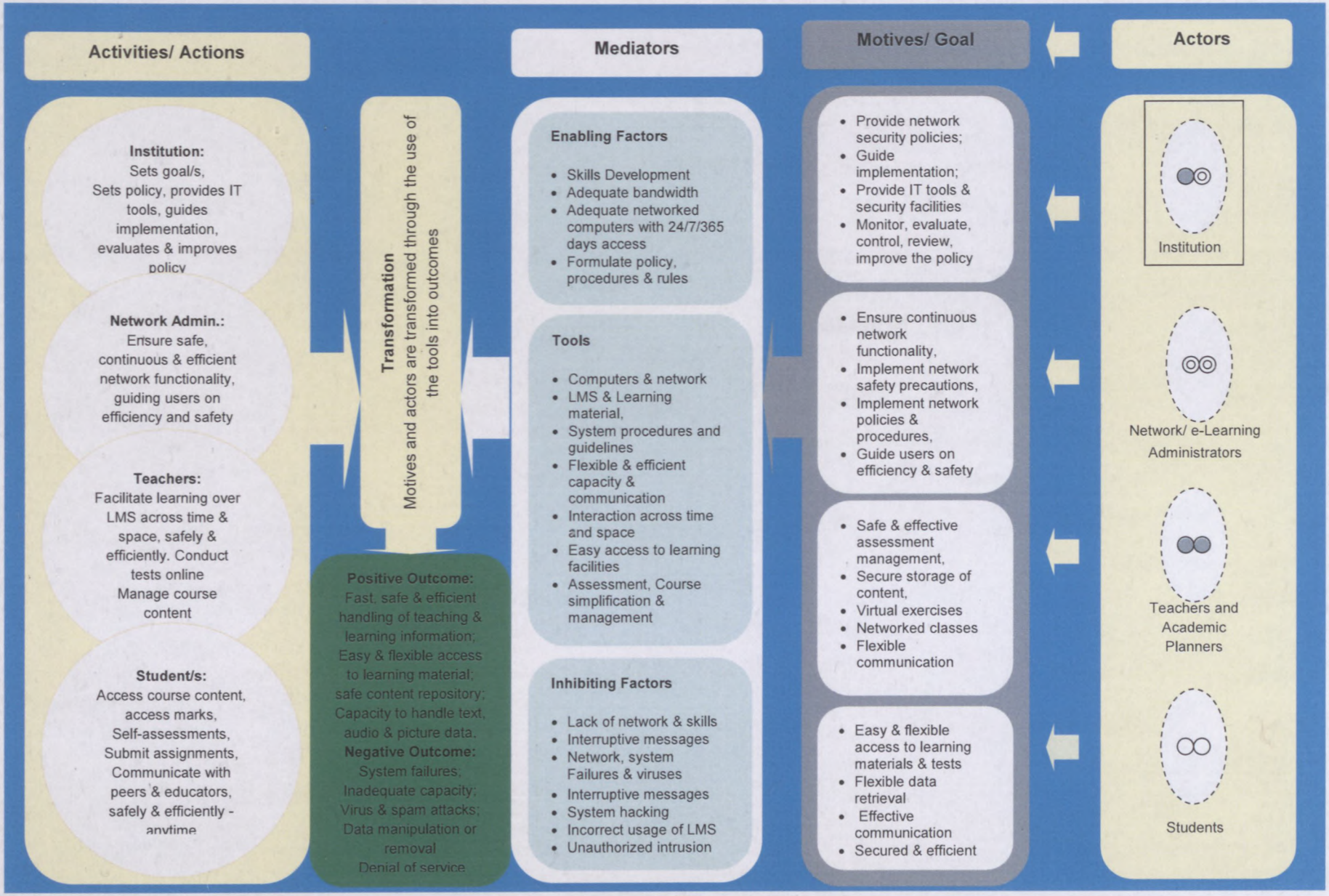


Figure 4: Work-Activity Framework for Security Analysis in e-Learning System (Mlitwa, 2011)

In this thesis, Figure 4 presents a security perspective of e-Learning systems using common AT key terms. On the framework Figure 4 there are four set of actors ranging from the institutional managers to students with goals performed on the system.

Main actors include Institutional managers in a form of institution. Their aims are to set goals that are specific, detailed, clear, and realistic for entire organizational; provide adequate, relevant IT tools that will help maintain, control; and evaluate the use of the network and its policy. The institutional managers need to carry out their respective using appropriate tools in their respective contexts to achieve goals. The second group of actors is IT/e-Learning administrators in a form of IT/e-Learning department which ensure continuous network functionality; implement network safety precautions, and guiding users on efficiently and safety of the system.

Other actors are teachers in a form of academic departments and students within the academic departments. The goals of teachers are to become effective and enhance teaching through the electronic medium; facilitate the learning through the LMS; conduct assessments securely; and store the content on the system. Finally, student's goals are to communicate efficiently; and easy access to the learning material stored on the system. Whilst the focus of the study is to understand security affects teaching and learning at CPUT, but results cannot be described without thorough considerations of enabling factors. However, the success and failure of all the actor's goals highly depends on the effectiveness of positive or negative mediators.

As shown in Figure 4, mediators are tools that enable or hinder the process within an activity system. Enabling mediating factors include skills development, adequate bandwidth, adequate networked computers with 24/7/365 days access, effective policy with clear rules and procedures as well as enforcement network policy. These factors could provide a positive outcome in the presence necessary tools to carry out activities. Tools include networked computers; learning material loaded on the LMS; clear system guidelines and procedures; flexible, efficient capacity and communication; interaction across time and space; easy access to learning facilities; and assessment.

In essence, positive enabling mediators provide ideal platform for actor's goals to be carried out. All actors using an e-Learning system require a certain literacy skill in order to perform their activities effectively. For example, for teachers to conduct online assessments on a secure environment they need to be trained on how to effectively use the LMS. They should be able to facilitate teaching on an LMS using both simple and complex methods.

In the case of CPUT, there is an existing LMS for teaching and learning but inhibiting factors cannot be ignored. Inhibiting factors include incorrect usage of LMS due to the lack literacy skills;

interruptive messages on the system; network failures due to multiple viruses; unclear network usage policy and guidelines; system hacking; lack of proper training for network users; unauthorized intrusion and access. Hindering factors within an e-Learning activity system leads to a negative outcome. For example, teachers cannot fully utilize the system if there is a lack of training programmes.

The framework on Figure 4 provided the direction on this study and has helped to conceptualize the objectives.

The concluding statement is presented on the section below.

2.5 Summary/Conclusion

This chapter presented the background to teaching and learning and the use of activity theory to analyze e-Learning systems in a security perspective. The background briefly included the e-Learning adoption and benefits that increases at a very rapid pace. Thus, e-Learning functionality continues to depend mostly on the use of ICT. Its dependence to ICT resources and Internet has exposed e-Learning systems (LMS) to illegal activities and security threats.

An activity theory adopted in this study addressed the research questions by identifying, describing, and interpreting the sociocultural elements related to security of e-Learning systems. It was also used to analyze different levels of interactions within an activity system and proposes that activities consist of processes both at the individual and social level, including the e-Learning security tools and artifacts that link the processes together. The theoretical background on this chapter has provided the researcher with the basis necessary to advance and conduct a research at CPUT and to understand the status quo of security in e-Learning systems. The e-Learning work-activity system is also used as a guide in the process of data analysis.

The following chapter discusses the research methodology that is addressing how the study is conducted.

CHAPTER THREE: RESEARCH METHODOLOGY

3. Introduction

This chapter presents research paradigms, the design and methodology used to address the problem as outlined in chapter one. The chapter is introduced, and the study located under the information systems (IS) research discipline in the introduction section.

The term IS can be understood both as a technical collection of information (including data) handling software, applications and systems, and also as an academic research discipline (Mlitwa, 2009, Peffers & Ya, 2003). In the first instance, technical practitioners, who often attach different interpretations to the term, use the term loosely. In most cases, the term is seen as a system of people, data records, and systematic activities that process the data and information in an organization (Clarke and Mayer, 2003). For many organizations, the term is used as a name for a department responsible for computers, networking and data management. As a subset of information technology, an information system (or computer-based information system) technically refers to specific software applications used to store data records in a computer system, and to automate information-processing activities of the organization (ibid).

As an applied discipline, Information systems embraces the means by which organizations and people use (ICT) computers to collect, process, store, use (analyze) and distribute information (UCT, online). For teaching and learning purposes (as adopted in this thesis), an information system is technically understood as a collection of information and data (in the form of learning content) handling software, networked teaching and learning interfaces, programs and procedures (Mlitwa et al., 2009). In whichever way the term is interpreted, it is commonly understood and pronounced as separate letters and as an abbreviation of the full phrase of an "Information System".

Therefore, this study involves people, information, processes (activity to develop or deliver a service) and Information Communication Technology as a platform and an enabler to carry out these services. IST (Information Systems and Technology) as per (MSIT, online) is the department that assists students with interest, not only in computer systems, but in the use of computer systems as a tool.

As a young academic and research discipline, an information system is still in the middle of the identity debate (Peffers & Ya, 2003). Researchers are divided on whether IS research is an independent discipline, or merely a multidisciplinary field. Dissidents cite IS reliance on other disciplines such as psychology, business and computer science for theories and methodologies

to dispute its maturity; and to critique IS as a dependent interdisciplinary field (Boland & Lyytinen, 2004).

When it first emerged from its mother discipline, computer science, into a new discipline in 1984, IS research largely followed the positivist theories and methodologies associated with the computer science discipline. In this instance, IS researchers often work towards generating findings that are immediately applicable in technical practice, mostly focusing on the technological rather than the socio-technical aspects, with less attention on the human aspect side of research (Bhattacherjee, 2012). This chapter discusses research paradigms in section 3.1. The research methodology is outlined in section 3.2, followed by the research design in section 3.3; data sampling and selection in section 3.4; data analysis in section 3.5; and research ethics in section 3.6. The chapter closes with a summary/conclusion in section 3.7.

3.1 IS Research Paradigms

Research paradigm refers to the methodology and a specific model adopted to conduct the research (Henning et al., 2004). Similarly other authors indicate that a paradigm states the aim of the study by finding the epistemological, ontological questions and methodological basics as well as study guidelines and restrictions (Guna and Lincon, 1994). However, the researcher explains her beliefs relating to the nature of knowledge and how knowledge is developed as an epistemological question of the study. With the ontological question, the researcher deals with the form, and nature of reality based on the phenomenon and subject under the nature of knowledge. The intention is to elucidate a clear approach in the research followed by an enquiry. Lastly, methodological basis focuses on research methods, and techniques used to carry out the study (ibid).

However, epistemology is a branch of philosophy with a focus on understanding the way of knowing. Emphasis is placed on studying knowledge, including that which is rooted in a methodology and theoretical perspectives, making a distinction between adequate and inadequate knowledge (Crotty, 1998). Epistemological positions vary between those who believe in the physical objective reality (realist ontology), proposing direct physical and objective methods of observation and a separation of the subject and the object - as the only valid way of getting to know (i.e. positivism), to those who believe in the relative (and inter-subjective) nature of reality (relativist ontology), where knowledge can be gained (and constructed) through engagement with, and interpretation of, the context (i.e. intepretivism) (Mlitwa, 2011). The type of knowledge under investigation in this study is content-based, inter-subjective and therefore, subject to interpretation by participants, which could be engaged through intepretivist (rather than positivist approaches). Between the positivist and interpretive paradigms stands the critical theory

approach with a focus on detailed critique of obscure social relations, with emphasis on emancipation (Takala, 2008). Focusing mostly on social, cultural and political issues tends to be the focus of critical research. The critical approach thus, serves more as a supplement rather than an alternative to the two paradigms. It, assumes that "social reality is historically constituted and that it is produced and reproduced by people" (Brooke, 2002:50).

3.1.1 Interpretive Research Paradigm

In general, interpretive studies aim to understand the phenomena through implications allocated by people to the research and interpretive methods in the IS field. As a result, these investigations attempt to find and interpret the meaning in the information system, and the way IS influences and is influenced by those meanings (Bhattacherjee, 2012). People tend to interpret every activity done during the IS process. Other researchers explain this approach as one that fully pays attention to the human sense density as the situation emerges (Cresswell, 2008; Kaplan & Maxwell, 1994). As used in these studies, actors which are research participants, aim to understand and make sense of every action done on various levels in order to accomplish a concrete output.

Schwandt (1994) argues that this approach primarily focuses on the meanings, and in order to understand explanations or definitions of a certain situation. The paradigm assumptions are that knowledge and meaning are acts of interpretation; hence there is no objective knowledge which is independent of thinking and reasoning humans. Similarly, it addresses the fundamental features of shared meaning and understanding, as well as being concerned with the objective reality it requires to reflect on the differences between the human meaning and sense making; and show variation in objective realities (William, 2003). In order to obtain qualitative data, to gain an understanding and meaning of everyday life of the actors that are studied, the researcher spends a period of time in a social setting while using relevant methods (Bhattacherjee, 2012; Neuman, 2006). The current study adopted the critical interpretive paradigm to investigate the status of e-Learning security at CPUT.

3.2 Research Design

In a practical research, as described by Bhattacherjee (2012), the term research design is detailed structure used for the collection of data. Its aim in scientific work is to provide an answer and a systematic process to the specific research. Research design focuses on bringing answers to a specific problem area with the supporting literature through the process of data collection, instrument development process and the process of sampling (ibid; Huck, 2012).

3.2.1 Research Methodology

This section discusses methodological approaches to investigate research problems. Babbie & Mouton (2001) explains a research methodology as a logical, organized execution and implementation of a research plan. Elements that make up a research methodology are strategies, techniques, methods and procedures used to carry out the process of design and implementation (ibid; Bhattacherjee, 2012).

In line with the positivist paradigm associated with natural sciences, quantitative research is concerned with the use of structured questions. It involves a very large number of respondents whereby expected responses or feedback could be predetermined and statistically analyzed (Gall et al, 2003; Cresswell, 1994). Surveys and laboratory experiments, among others are the most commonly used research techniques in this design. Formal methods such as econometrics and numerical methods e.g. mathematical modeling can also be used in this method. By definition, a measurement must be objective, quantitative and statistically valid. For example, variables are used to measure aspects of the research problem (Barbie & Mouton, 2001; Huck, 2012).

The aim of this study however, was to understand the extent to which security measures associated with e-Learning practices are implemented at e-Learning administration, at IT network administration, at academic planning, at the educator and at student levels. This involves an understanding of the level of e-Learning related security awareness that exists within these departments that use e-Learning facilities at CPUT. This implies working within a context-based area of study where unpredictable inter-subjective circumstances and the context constitute the bulk of the data. Under this investigation therefore, it would have neither been logical nor practical to separate the researcher, the subject and the object of investigation. Its origins are qualitative (descriptive and explanatory), which calls for qualitative analysis and interpretation methods and techniques which are specifically discussed and adequately elaborated on section 3.2.4. of the study.

3.2.2 Qualitative Research Methodology

This research design enables researchers to simultaneously study social and cultural phenomena. Some researchers define qualitative research as being multi-method in focus, involving an interpretive, naturalistic approach to its subject matter. The focus of this methodology is on studying things in their natural settings, attempting to make sense of or interpret phenomena in terms of the meanings people bring to them (Bhattacherjee, 2012; Denzin and Lincoln, 1994). Qualitative research methods are designed to help researchers understand people, the social and cultural contexts within which they live.

As opposed to quantitative data, qualitative data allows a researcher to obtain a broader understanding of the social problem in that particular social setting in which the results are interpreted (Leedy & Ormrod, 2005; Cresswell, 2008). Most commonly used qualitative research methods are action research, case study research and ethnography (Klein & Myers, 1999). A case study method which was used in this study is discussed in detail in the sections that follow.

3.2.2.1 A Case Study and Its Usage

Yin (1994: 23) defines a case study as

"...an empirical enquiry that investigates a contemporary phenomenon within its real-life context, when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used". With regards to the real life context, this study sought to investigate the security aspect LMS usage in a direct operational context at CPUT. This implies understanding the network, usage objectives and processes of e-Learning administrators, courseware developers, educators and learners – in their real-life operational environments. For this reason, a case study was more than ideal, in that it allowed the researcher to select a case of the institution, and select respective samples within these categories of stakeholders (actors) in order to carry out an informative investigation. The current study also sought data from different stakeholders within the e-Learning activity system, making it inappropriate to follow methods that could separate the subject of investigation from the context.

A case study is a detailed examination of a single example of a class of phenomena or as a research design, which takes a single case as its subject. Cases may be defined from individual units to group/s including organizations (Bhattacherjee, 2012; Baxter & Jack, 2008). As emphasized in the definition of a case study that it is significantly appropriate *"when the boundaries between phenomenon and context are not clearly evident"* (Yin, 1994: 23), a case study was clearly relevant for this study. In terms of the current study, multiple sources of information were used to gather data. The sources ranged from the CTS departmental head, CTS technicians, academics and students who are directly involved with the LMS.

In effect, considering the significance of this strategy, the case of CPUT is selected with the purpose of understanding what, why and how the security aspects of e-Learning systems are within the University.

- **CPUT Case Setting**

This study represents a case of CPUT, Cape Town, Western Cape Province, in South Africa. CPUT emerged from the old Cape Technikon and Peninsula Technikon in the year 2005. After the merger of the Peninsula and Cape Technikons, it became a University of Technology, joining

other traditional universities in the province which are: University of Stellenbosch (US), University of the Western Cape (UWC) and University of Cape Town (UCT).

CPUT is currently operating at eleven campuses in the Western Cape which are Cape Town, Bellville, Mowbray, Granger Bay, Worcester, Tygerberg, Thomas Pattulo, Grooter Schuur, MARC, Athlone and Wellington. Some of these campuses offer almost the same qualification whereas some of the campuses work with their specializations for example, the department of information technology is represented in the Cape Town campus only under the Faculty of Informatics and Design.

The university adopted the proprietary LMS (WebCT) in 2001 to enhance their teaching and learning, which was later changed to Blackboard in 2011. This study was conducted in two campuses where IT was initially offered because it is the first department that should keep up with the latest technology. Data sampling was done on these two campuses to gather information from the relevant participants.

3.2.2.2 The Sampling Process

Sampling is a technique of choosing a relevant group from a research population, for the purpose acquiring data (Bhattacherjee, 2012; Mugo, 2002). Whilst a sample is selected from a relative population, a population is the group of interrelated organisms inhabiting a given area or group of individuals, or objects from which the sample size could be selected (ibid). A population can be too large, time consuming, costly and not accessible to the researcher (Labovitz & Hardgedom, 1981; Cresswell, 2008), so a sample is needed.

There are two types of sampling methods, viz. the probability and non-probability sampling methods. Probability sampling starts by deciding on the research population to be used. That could be persons on a certain age group (Barbie & Mouton, 2004). Random sampling takes various formats, including simple random, stratified, systematic, and cluster samplings.

Every unit in a research population has an equal chance of being selected into the sample, meaning that a researcher would need to know the quantity and location of all units of a research population in order to facilitate the selection. This method utilizes some form of random selection whereby a researcher has to set up the process that assures the equality of probabilities of various units in a given population (Neuman, 2006). Probability sampling works well with studies that seek to gather information from all participants; however, this was not the case in the current study. Therefore, instead of targeting numerical quotas, the research population in the current study was of such a nature that for the purpose of the study, it was adequate to determine the

characteristics and ideal numbers of participants. Purposive sampling discussed in section 3.2.3., was applied.

3.2.3 Purposive Sampling

This sampling technique is used when a researcher seeks to access a particular subset of participants, or a sample, from a research population (Barbie & Mouton, 2004; Bhattacherjee, 2012). A researcher starts with the purpose in mind, the experience they have, as well as the recent findings to achieve participants by regarding the findings as the representatives of appropriate population (Huysamen, 1994). Thus the sample is selected to involve people of interest and to further exclude those who do not fit the particular purpose. Barbie and Mouton (2004:166) suggests that *"it's appropriate for you to select sample on the basis of the population, its elements, and the nature of the research aims"* therefore purposive sampling pays more attention to the sample of participants that have knowledge about the subject of the study, than to those do not. In this technique, a researcher selects a sample based on who they think would be appropriate for the study. This technique is primarily used when there are limited numbers of people that have expertise in the area being researched (ibid).

The purposive technique was adopted in this study because the researcher is seeking more information from the departments that are directly having an impact on, and use of, the e-Learning and networked systems. In addition to that, the researcher considered that the mentioned departments would be more appropriate than others, and would be able to give concrete information based on their experiences of, and observation on, the security of the e-Learning system.

On this study, sampling has been done to the number of various stakeholders that uses the networked systems. The purpose of this sampling is to gather information from a certain population. The information gathered is used and analyzed to come up with the findings of the study. This was done with the purpose of obtaining the richest possible data that could be analyzed to meet the current studies objectives. All these participants were selected from CPUT in the Western Cape Province which was selected as a representative sample of the study. It was chosen primarily, for the fact that it is a university of technology among other universities in this province. Secondly, the researcher works at this university, and uses the current LMS to enhance her teaching and also familiar with conditions. For this reason, it was going to be more practical for the researcher to engage with the departments using the LMS. Table 3 outlines the sampling process followed in this study.

Samples were drawn from the CTS department, IT and Public Relations academic departments in two CPUT campuses (Bellville and Cape Town), in the Western Cape, South Africa. However,

participants were identified on the basis of their network, LMS roles and knowledge in their departments within the university.

Table 3: Sampling

Theme of Investigation	Data Sources	Units of Analysis	Units of Observations		Selected Sample	Data Collection Methods
• Background, methodology, theory	Literature	Books, Journals, Internet	Security, e-Learning, Methodology, Theory Books & Journals. Online Journals & CPUT LMS website.			Read, Write, Analyze
• Security threats on the network (in general)	• IT Infrastructure & Networks dept. • Academic depts.	• Network & end-user support division • System users: IT & Public Relations depts.	• CTS official head • Teachers/ Academics • Students	CPUT (CT*)	1 8 16	Interviews Interviews 2 focus groups of 8 students
• Security threats on e-Learning systems	• IT Network (including e-Learning) dept. • Academic depts.	• Network & end-user support division • System users: IT & Public Relations depts.	• CTS official head • Teachers/ Academics • Students	CPUT (CT*)	1 8 16	Interviews Interviews 2 focus groups of 8 students
• Availability of security awareness programmes for network users (including e-Learning system users).	• IT Network (including e-Learning) dept. • Academic depts.	• Network & end-user support division • System users: IT & Public Relations depts.	• CTS official head • Teachers/ Academics • Students	CPUT (CT*)	1 8 16	Interviews Interviews 2 focus groups of 8 students
• Status of network security measures	• IT Network (including e-Learning) dept. • Academic depts.	• Network & end-user support division • System users: IT & Public Relations depts.	• CTS official head, • Senior Technician • Teachers/ Academics • Students	CPUT (CT*)	1 1 8 16	Interviews Interviews Interviews 2 focus groups of 8 students
• Extent of network security implementation	• IT Network (including e-Learning) dept. • Academic depts.	• Network & end-user support division • System users: IT & Public Relations depts.	• CTS official head, • Senior Technician • Teachers/ Academics • Students	CPUT (CT*)	1 1 8 16	Interviews Interviews Interviews 2 focus groups of 8 students
• LMS usage & capabilities	• Academic depts.	• System users: IT & Public Relations depts.	• Teachers/ Academics • Students	CPUT (CT*)	8 16	Interviews 2 focus groups of 8 students per group
Explanatory Notes: *CT = Cape Town *BLV = Bellville				**Sample Total**	**26**	

The sampling process in Table 3 is presented according to the issue of investigation, followed by the identification of the source of data for each of the theme (issue) of investigation. With the exception of the background, methodology and theory insight, there were six themes (issues) of investigation for which, data sources (including units of observation) had to be identified and samples selected. Such themes of investigation are: security threats on the network in general; security threats on e-Learning systems; the availability of security awareness programmes for network users (including e-Learning system users); the status of network security measures; extent of network security implementation; and LMS capabilities and usage.

- **Security Threats on the Network in General**

IT Infrastructure, network and academic departments were selected and used as data sources for this theme. These sources were selected because of their extensive knowledge and experience relating to e-Learning systems at CPUT. A number of units of analysis were selected varying from the network, end-user support divisions and system users in IT and Public Relations departments. The criteria was that the department should be rendering computer and internetwork services to users (students, academics and non-academics) in CPUT at large. Within these departments, CTS official head, 8 teachers and 16 students were identified as unit of observations at CPUT, Cape Town campus. The assumption for teachers was that academics would be using networked systems for their daily operations. The idea was to identify educators who were the most frequent users of e-Learning systems, on the basis that they would be familiar with the functioning of the system and its process challenges. On this aspect, 5 teachers from the IT department, and 3 from the PR department who met this criteria were selected. In this respect, semi-structured interviews were used as tools to collect data.

The criteria for students were based on level of study, for example, focus was on students currently enrolled for their first and second year within the IT and PR departments, where electronic systems are a significant part of curricula. The idea was that learners would be familiar with conditions of e-Learning environment and its security related challenges at CPUT. Sixteen students were selected for 2 focus groups composing of 8 students each. With students, focus group interview technique was used to gather data. Focus groups were conducted in Cape Town campus, Commerce building, room 1.65, where students were

divided into sets. These sets were representing first and second year registered students so as to share their views about the theme.

- **Security Threats on e-Learning systems**

IT network and academic departments were identified as ideal sources of data for this theme. Within the IT network department, units of analysis are network and end-user support divisions of which, the unit of observation was the CTS official head. CTS departmental head was selected for his direct involvement in network and e-Learning systems. In addition, for the level of understanding and direct experience on the CPUT systems. Within academic departments are system users such as teachers and students in the IT and Public Relations departments. Teachers and students were selected because they directly use the LMS for teaching and learning. The same number of participants, and data collection methods were selected and used as reflected on the security threats on the network in general theme.

- **Availability of Security Awareness Programmes for Network Users**

IT network including the e-Learning department and academic departments were identified as ideal sources for this theme. Units of analysis within the IT network department are network and end-user support division with CTS departmental head as the units of observations. The departmental head was selected due to their practical and concrete knowledge about the availability of security awareness programmes relevant for network users and e-Learning system users. Within the academic departments, systems users which are teachers and students were identified as units of observations. Teachers and students were selected because of their knowledge and usage of the network.

In this theme, the same procedure as mentioned on the security threats on e-Learning system theme, applied when identifying and selecting the units of analysis and observations, the number of participants and the collection methods. All these participants were selected from the Cape Town campus.

- **Status of Network Security Measures**

The same strategy of identifying sources of data, units of analysis and units observations as used on the preceding themes applied. In this case, a senior technician was also included in the units of observation, to offer insight from the network and end-user division perspective. The technician was selected on the basis of his level of expertise, day to day operations and measures they apply on the network.

- **Extent of Network Security Implementation**

The same procedure applied (as mentioned on the status of network security measures) in this theme when identifying data sources, units of analysis, units of observations, number of participants per campus and the method of collecting data.

- **LMS Capabilities and Usage**

On this theme, the researcher has identified only academic departments as the data sources. Units of analysis selected are system users which are teachers and students in both the IT and PR departments. The same procedures of selecting a number of participants and collection methods for both teachers and students have been used. Section 3.2.4 broadly explains how data collection methods have been used in the study.

3.2.4 Data Collection Methods

In this study, both interviews and focus groups were used to gather empirical data from various participants. These data collection techniques were used to gather data from the CTS senior official and technician; teachers and students at CPUT. Data collection techniques are explored below.

3.2.4.1 Interviews

Semi-structured face-to-face interviews were conducted with the CTS senior official, technician, teachers, as well as students to allow them to raise points not considered by the researcher. The interviews were semi-structured as to grant respondents an opportunity to mention certain points that the researcher did not consider. This type of interview has helped to gain concrete information in an easy relaxed environment. Nine is the total number of face to face interviews conducted to obtain better understanding about the status quo of e-Learning security awareness by LMS users (see Table 4). These face to face interviews were done with individuals in a pleasant and calm environment. They resulted to meaningful discussions because all the respondents were exposed to the LMS at CPUT.

Table 4: Number of respondents for Interviews

	CTS Departmental Head	CTS Technicians	Teachers	Totals
Face to face	1	1	7	9
Totals	1	1	7	9

Table 4 presents the total number of respondents participated. The researcher interviewed ten participants which are CTS departmental head, a technician, and seven academics. However, the procedure for conducting interviews is explained on the section below.

Interview Procedure

All participants were selected and contacted to request for the permission to part take in the research. After respondents have agreed up on the appointment, the researcher sent an outline of the interview with the list of research questions to the participants at least a week before an appointment date. Respondents were given a research consent letter (see Appendix C) with the information that the researcher wanted to cover with a brief introduction to the study, research aims as well as agreement to participate.

A small Sony digital recorder has been used to record the interviews. It was placed in an unobtrusively area as possible. However, after a moment most participants stopped being hesitant about being recorded. Most of the interview duration lasted for thirty minutes to forty five minutes. The researcher preferred to just listen rather than write due to nerve damage which makes it difficult for her to write quickly and clearly, and this may have contributed towards a more sympathetic attitude to being recorded. The interviewees were told that the aggregation of data would cut down any possibility of the subjects being identified. Data captured and collected during the interviews was later transcribed by the researcher.

Another data collection method used by the researcher is the focus group interview which is outlined below.

3.2.4.2 Focus group interviews

However the difference is that, focus groups "enable members to share their experiences" to clearly understand a specific topic in a cool and non-threatening environment (Bless & Smith, 1995: 113). This technique was used to collect data from multiple respondents at a time. In this study, focus groups had maximum of four participants (See Table 5).

Table 5: Number of focus group respondents

	Focus Group 1	Focus Group 2	Focus Group 3	Totals
No of Students	4	4	4	12
Total	4	4	4	12

Table 5 shows the total number of student focus group participants identified. However, the study had three student focus groups from full time and part time offering type. Students were in groups of four's per group. Questions used during the process were prepared to measure variables which were identified in the operationalization process.

3.2.5 Operationalization of Variables

Operationalization is the development of specific research procedures (operations) such as survey questions, experimental protocol, interview schedules, observation protocol, etc, that result in empirical observation representing those concepts in real world (Babbie & Mouton, 2001). This indicates how variables are defined and measured in the study. List of questions were prepared to measure variable(s), after operationalization concepts have emerged. Operationalization of e-Learning security awareness variable is presented on Table 6.

Table 6: Operationalization of a variable: LMS Security Awareness

Measure / Variable	Attributes	Indicators	Units of Observations	Tools
LMS Security awareness by • CTS department	• Enabling security policies & procedures • Active organizational structure for system & network security • Availability of security tools, infrastructures & user awareness programs • Sound security practices & strict enforcement measures	• There is a clear security policy, user manuals • Clear roles & responsibilities for administrators, technicians & users • Up to date antivirus software, firewalls, servers, hardware & software as well as other related programs • Correct usage of username and password • Training programmes & workshops • Electronic reminders on password changes • Active compliance monitoring system • Proper usage of security practices	• Departmental head	• Interviews
• IT & PR departments	• Adequate usage of available programmes • Adequate user awareness programs • Sound security practices	• Adequate knowledge about LMS security & its implications • Correct usage of username and password • Active compliance monitoring system • Proper usage of security measures	• Academics	• Interviews
• Learners	• Adequate usage of available programmes • Adequate user awareness programs • Sound security practices	• Adequate knowledge about LMS security & its implications • Correct usage of username and password • Active compliance monitoring system • Proper usage of security measures	• Students	• Interviews & focus groups

Table 6 represents operationalized e-Learning security awareness variable within various departments such as CTS, IT and PR departments. In this study, the LMS security awareness refers to user's knowledge and understanding about the LMS. In addition, it refers to the LMS capabilities and usage including what they use it for, application programs used to enhance teaching and learning. Information about the level of awareness by CTS departmental head, academics and students was gathered through the use of interviews and focus groups. Within this variable, respondents were asked whether they use the LMS for any purpose, if they use it, what do they use it for and fluency for the usage. They were also asked to indicate the level

of their access rights to the system.; use of synchronous and asynchronous communication capabilities; ability for an LMS to handle all data types as well as application programs used by academics for their teaching. That is how phenomenon of security LMS awareness was operationalized and measured in this study. Operationalization of security measures against unauthorized access, access hindrances and data handling failures are presented on Table 7

Table 7: Operationalization of a variable: Security Measures

Measure / Variable	Indicators	Units of Observations	Tools
Access control – measures against: • Unauthorized access	• Renewal of password rules to enforce strong password creation criteria to avoid passwords guessing. • Clear password policy to implement & maintain the duration of the active password • Relevant access rights to allow access to users • Sniffers to monitor the usage of the system & modification or removal of data	• Departmental head • Academics • Learners	• Interviews & focus groups
• Access hindrances	• Adequate bandwidth & strong network strength carry all the traffic • Antivirus software to mitigate threats • Regular network & system maintenance for timely effective access • Proper user literacy skill to effectively use the system • Acceptable infrastructure to provide a better platform for users to reduce slow network & freezing computers	• Departmental head • Academics • Learners	• Interviews & focus groups
Measures against • Data handling failures	• Acceptable capacity to develop, exchange & handle diferent data formats • Adequate & necessary programs to facilitate multi format file • Adequate bandwidth to carry converged data • Adequate infrastructure to support planned delivery system.	• Departmental head • Academics • Learners	• Interviews & focus groups

Table 7 represents an operationalized e-Learning security measures variable within CTS, IT and PR departments. Information about these variables was collected from the CTS departmental head and academics using interviews as well as students using focus groups. Thus, security measure variable consists of security measures against unauthorized access, access hindrances, and measures against data handling failures as well as the extent of their implementation. The extent of implementation of these measures is considered as the frequent maintenance of the e-Learning system against hindrances.

In this study, security measures refer to practical precautions to avert www network related risks to information over an LMS. Within this category, respondents were asked the ways of protecting critical information on the system; composition of their passwords; duration of the passwords to expire; indicating ideal measures for protecting critical information as well as extent of implementation of security measures against hindrances.

3.3 Data Analysis

Data analysis according to Neuman (2006) refers to the interpretation of either quantitative or qualitative elements of information lacking a meaningful order into significant and meaningful knowledge. Whilst, quantitative data analysis is mostly developed and shaped on applied mathematics, whereas, qualitative data analysis is mostly inductive and does not pull from a very large number of proven knowledge from both statistics and mathematics (ibid). The distinction is made between quantitative and qualitative data analysis methods. As an interpretive study working with the qualitative data, it is appropriate for this research to adopt the qualitative data analysis methods.

Qualitative data analytical methods enable the analysis of descriptive and explanatory content in the form of "*words, ideas, meaning, pictures, symbols, themes or any message that can be communicated*", including text which represents anything serving as a medium of communication such as written, visual, or spoken (Neuman, 2006: 322). Qualitative analytical methods include discourse and content analysis (Babbie & Mouton, 2004). The content analysis explained below is used as a technique to gather, analyze data in this study.

3.3.1 Content Analysis

Qualitative content analysis is referred to as "*a research method for subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns*" (Hsieh & Shannon, 2005, 1278). It further focuses on themes, outlining the range of meanings of the phenomenon. In this instance, qualitative raw data is grouped into themes for further translation into more meaningful information. The qualitative nature of data in the current study required such an analytical process. For example, themes of the current study are developed based on the objectives and goals of the study and according to the concepts of the theoretical framework.

In effect, the study used the framework on **Error! Reference source not found.** to outline themes. **Error! Reference source not found.**, demonstrates the work-activity framework for e-Learning Systems, in a security perspective as an activity system. In this sense a framework is made up of actors, goals/motives, activities, mediators, transformation and outcomes. As used in this study for example, four levels of actors are institution, network administrators, academics and students. All of these actors have goals to achieve towards the system. However, those goals act as one of the core themes to be identified in the data transcripts.

In addition, activities and mediators also add the most important theme in this study. For example, outcomes of these activities depend on the mediators used. These mediators use tool, enabling factors and inhibiting factors, however, for an outcome to be positive, it has to get an influence from the proper adequate tools and enabling factors (See **Error! Reference source not found.**). However, list of coding categories used were derived from the activity theory framework. Clearly all the themes from the activity system were used to inductively categorize data and group similar content in all transcripts, into similar themes by coding, and constantly counting and checking the number of times a word appear on one's transcript (Hsieh & Shannon, 2005).

3.3.2 Data Analysis Process

This study used content analysis and AT to analyze the collected data through face-to-face interviews and focus groups. Engerstrom (1993) explains that AT is mostly used to examine an event in its natural setting as an activity system. The researcher has used this theory as a lens to investigate the security aspects of e-Learning systems at CPUT. In addition, a framework on Figure 4 shows activities by actors who work under common rules, guidelines, conditions known as mediators to pursue a common objective, through the use of tools (Korpela et al., 2002).

After completing the process of transcription, color coding process followed where transcripts were used to identify study keywords, concepts and themes. The process of coding started after transcription was completed Keywords that belonged to the same theme were grouped together and ultimately, research findings were discussed. The researcher further scanned through data on the electronic transcripts, identifying keywords, themes and concepts using color coding. Likewise, research questions from interviews were also color coded, same concepts belonging to the same theme together and ultimately discussion of research findings began.

3.4 Ethical Considerations

Interviews were held in adherence with the guidelines of the Post Graduates Ethics Committee of the Cape Peninsula University of Technology, as well as of the respondents from institutions. Permission to conduct interviews was sought from respondents, and their institutions. The purpose of research and analysis of findings is communicated to respondents. Identity of respondents is treated with strictest confidence is therefore, not

disclosed except in cases where permission was obtained from respondents. In this instance no reservations on confidentiality matters were raised, and even though participant identities are concealed in this study, this is done as a mere precaution (and adherence to ethical good practice) rather than due to the concerns of participants.

3.5 Research Summary/Conclusion

This chapter gave a broader insight about research methodology used in the thesis. Thus, it briefly explained research approach, designs, and methodology suitable for the current study. In the same light, possible ways of conducting empirical data were discussed and the selection of the method for the current study was motivated for, and elaborated. The logic for selection of the specific approach, design and methods appropriate for this study were outlined. Various researchers showed their views about commonly used approaches. Whilst critical paradigm as concerned with prevailing social power structures and aims at empowering its human research subjects, interpretive approach seeks to understand social member's definition of a situation (Schwandt, 1994).

The overall methodology for this study is based on social and cultural phenomena. The researcher studied things in their natural settings, to interpret the phenomena in terms of the meanings people bring to them.

The nature of the study worked well using an inductive form of reasoning implying that literature, theoretical work and data were used to offer new insight, rather than using a theory to predict the findings (Babbie & Mouton, 2004).The chosen approach largely depended on the subject and the field of the study.

The following chapter (chapter four) discusses the findings of this study.

CHAPTER FOUR: RESEARCH FINDINGS

4. Introduction

The use of ICT and learning management systems has been on the rise in academia at the dawn of the 21st Century. The problem however, is that security threats have hindered efficiencies and the educational benefits of these practices. For this reason, the status of security readiness of the CPUT e-Learning systems was explored in this study. The idea was to improve security practices, systems efficiency and ultimately, teaching and learning outcomes for and among the CPUT e-Learning system users such as academics, students, CTS administrators as well as technicians. To achieve this objective, samples were drawn from the populations of academics, CTS administrators, technicians and students within the university, to find out the level of security awareness held by e-Learning users, the awareness programs in place for users, the current security threats to system; the measures that are in place to deal with the existing threats and the extent to which these measures are used. Activity theory was used to formulate an analytical framework, the Work-Activity Framework for security analysis in an e-Learning system Figure 4 towards this end.

The analytic framework in Figure 4 presents a security environment in an e-Learning platform – as an activity system composed of interrelated parts, actors and activities joined together by a common goal. An ideal security environment in e-Learning according to this framework should have actors with goals.

As presented in the work-activity system framework Figure 4, actors are: the institution (CPUT in this case); IT/network administrators; teachers or academics; and students. All these actors ought to perform various activities with the e-Learning system in order to accomplish their specific individual goals. In an ideal e-Learning space for example, an institution as an actor would formulate clear, comprehensive, detailed, inclusive network security policies, rules and procedures to sustain, evaluate and expand usage of the connected systems. In addition, network usage policies, rules and procedures should apply to all e-Learning users for compliance purposes. This actor should also enforce constant implementation and practice of these rules by all affected users, while at the same time maintaining the flexibility to update the technology. Administrators should ensure that the networked system operates effectively and efficiently without either interrupting the network users, or neglecting thorough and

adequate implementation of network precautions when guiding users to the secure and protected usage of the internetworked system.

Likewise, teachers should be able to use the same platform to store and retrieve the learning content securely; knowing that the platform facilitates learning by delivering the learning content in a networked environment in a timely fashion. Teachers should also be able to plan, create, edit and activate online assessment in a highly secured environment without compromising confidentiality, integrity and availability of such online assessments. In the same way, students should have unlimited 24/7/52 access to view and retrieve the stored learning material and assessments without any difficulties.

Students and teachers should be able to access the e-Learning system at their convenience, with no space and time limitations. However, for these activities to happen, the presence of mediators is necessary to perform the tasks that are necessary in order for the various actors to achieve their goals for the learning management system. Even though there are positive influencing mediators such as (adequate networking tools, literacy etc.) there are still negative inhibiting mediators such as (network failure, lack of skills, interrupting messages etc). An LMS transforms activities based on the enabling or hindering mediators and the existing tools to attain an outcome. In this case, an actor can only get a positive outcome through the use and presence of positive influencing mediators, but when these are absent, an undesired outcome may materialize. The framework Figure 4 explains in detail how the transformation of activities by mediators can produce a positive or a negative outcome.

This chapter presents the findings from the analysis of the data collected on section 4.1.

4.1 Research Findings

The study aimed to investigate security issues of e-Learning systems in Higher Education Institutions in South Africa using the CPUT case study. The main question was to understand whether, and to what extent LMS users (academics, students) are aware of, and affected by, security related aspects of the local system. To address this question, a purposive sampling technique was used to select participants among lecturers and students within the departments of Information Technology (IT) and Public Relations (PR) within the faculty of Informatics and Design (FID) at the Cape Town Campus. Table 8 outlines the sample and response rate of participants. Interviews with the participants were conducted during October

and November 2010 with seven academics, twelve students, CTS departmental head and CTS technician, as shown on Table 8.

Table 8: Number of Respondents

Number of Respondents							
Institution	**FID Departments**	**No. of Teachers**		**No. of students**		**CTS Technician &Administrators**	**CTS Technician &Administrators**
CPUT, Cape Town, Campus		No. of Selected	No. of Participants	No. of selected	No. of Participants	No. of selected	No. of Participants
	IT	5	5	12	12	3	2
	PR	3	2	4	0		
Total no. of participants		8	7	16	12	2	

Table 8 shows total of 8 IT academics, IT students and CTS administrator/ technician; whereas 7 for PR academics and none for PR students due to their unavailability because of busy schedule.

To analyze the findings, the main question of the study was divided into four themes – with related sub-questions. The first theme related to the level of LMS security awareness by users; awareness of existing programmes; existing security threats security measures and the extent of implementation of security measures.

Table 9 shows the status of security on the e-Learning systems at CPUT – from the academic perspective. This is followed by the students' perspectives in Table 10 and those of CTS administrators and technicians in Table 11. The content of findings in each table is then discussed in detail in section 4.3 below the three tables.

Table 9: Academic Experiences on LMS Usage – Security Perspective

Participants	How is the LMS Awareness (usage & capabilities)	What are the existing security (LMS) awareness programs, rules & procedures	What are the existing Security Threats and hindrances	What are the current security Measures	Explanations
Academics	• Very limited awareness about LMS & its capabilities on data formats (MM_IT22, MN_IT43, Mak-IT25) • Very limited usage of LMS (MN_IT21, Mak-IT7, MB_PR2)	• No specific awareness programmes (PR_TND40, MB_PR49, RT_IT 119, CST_IT81). • Academics are also not attending LMS training sessions (MM_IT10, PR_TND40)	• System inconsistent (Mak-IT7, RT_IT14,CST_IT7) and slow (CST_IT21, MB_PR25); • System often freezing (Mak-IT39, RT-IT10, CST_IT7); • Unstable network (CST_IT73, Mak-IT54); • Intrusive pop-up messages (MB_PR30, PR_TND99); • Multiple viruses (CST-52); • Unauthorized intrusion into LMS (Mak-IT2); • Unexpected service (access) denial (MB_PR1) • Frequent sharing of login details (RT_IT2, RT_IT4)	• Use of monthly renewable systems access codes with 6 alphabets only (MM_IT10, RT_IT45, MB_PR5); • However, this is not efficiently enforced as some academic never change LMS passwords (CST_IT17, MB_PR4) • There are Anti-virus programs (with frequent update cycles). However, academics label these programs as ineffective (MB_PR28, RT_IT 70, Mak-IT50, Mak-IT51, CST_IT55, PR_TND40)	*Limited Awareness:* • Academics hardly attend LMS training or still a beginner (MM_IT10, PR_TND40) *Limited Usage:* • LMS not secure to be used for assessments (PR_TND65, PR_TND31, RT_IT56, MB_PR 2); • System inconsistency discourages usage (Mak-IT7, RT_IT14,CST_IT7). Network is also unstable (CST_IT73, Mak-IT54) and slow (CST_IT21, MB_PR25); • It is also impossible to use the system when there is a denial of service (access failures) (MB_PR1). *Lack of Security Awareness Programmes:* • Specific reasons are unclear. Speculations are that users are assumed to be aware, and that specific measures are unnecessary. *Existing Security Threats:* • Limited security awareness (and awareness measures) (MM_IT22, MN_IT43, Mak-IT25). • Ineffective anti-virus software tools (MB_PR28, RT_IT 70, Mak-IT50, Mak-IT51, CST_IT55, PR_TND40) • Poor security enforcement measures (CST_IT17, MB_PR4) • Outdated infrastructure and poorly (MB_PR25) • Coordinated networking practices (CST_IT73, Mak-IT54) *Limitations in Security Measures:* • Unenforced password criteria (MM_IT10, RT_IT45, MB_PR5); • Inefficient usage of password (CST_IT17, MB_PR4) • Ineffective anti-virus programs (MB_PR28, RT_IT 70, Mak-IT50, Mak-IT51, CST_IT55, PR_TND40)
Exploratory Notes: * Interviews were done in CPUT, Cape Town Campus with all participants in October/November 2010					

Table 10: Students Experiences on LMS Usage – Security Perspective

Participants	How is the LMS Awareness (usage & capabilities)	What are the existing security programs, rules & procedures	What are the existing Security Threats and hindrances	What are the current security Measures	Explanations
Students	• Limited awareness about LMS (ABO17, MON114, MON116, MON145, ABO31) • Very limited usage (BNJ102, BNJ113, BNJ119, BNJ111, BNJ112, DVD-2n159)	• No specific awareness programs(DVD-2n108, BNJ125, MON154, MON155, MON156 MON157, MON158, MON150, DVD-2n183, ABO35) • Students are also not attending LMS training sessions (MON119, BNJ86, BNJ91, BNJ85)	• Unexpected service (access) denial (MON127, MON83, MON75, MON120, MON49, BNJ4, DVD-2n27, DVD-2n26, DVD-2n26, DVD-2n 32, DVD-2n29) • Limited LMS features usage by academics (MON123, MON131) • Unattractive user interface (MON109) • Frequent sharing of login details (DVD-2n 39) • Software incompatibility (BNJ43; DVD-2n37; DVD-2n 45) • Multiple viruses(DVD-2n 72, (DVD-2n60) • System inconsistency (DVD-2n 205, DVD-2n 90, DVD-2n 87, DVD-2n 223, DVD-2n 222, DVD-2n 118, DVD-2n 112) • Intrusive pop-up messages (BNJ76, MON99)	• Use of system access code with 6 numbers only (BNJ19, BNJ20, BNJ22, DVD-2n21, DVD-2n24, MON23, BNJ21) • Student never changed LMS password due to inefficiently enforcement (MON29, MON28, MON32, BNJ26, BNJ 25, MON30, DVD-2n203)	*Limited Awareness* • Students never attended LMS training or introduced to use LMS (MON119, BNJ86, BNJ91, BNJ85) *Limited Usage* • It is no possible to use system when there is denial of service (MON127, MON83, MON75, MON120, MON49, BNJ4, DVD-2n27, DVD-2n26, DVD-2n26, DVD-2n 32, DVD-2n29) • System inconsistency hinders the usage (DVD-2n 205, DVD-2n 90, DVD-2n 87, DVD-2n 223, DVD-2n 222, DVD-2n 118, DVD-2n 112) with network congested with viruses(DVD-2n 72, (DVD-2n60) • Limited usage of LMS features by academics (MON123, MON131) *Lack of Security Awareness Programs:* • Students were not introduced to any security related awareness programs, and there are no specific reasons indicated *Existing Security Threats* • Constant system cut-offs (MON127, MON83, MON75, MON120, MON49, BNJ4, DVD-2n27, DVD-2n26, DVD-2n26, DVD-2n 32, DVD-2n29) • Academic illiteracy (MON123, MON131 • Poor LMS interface (MON109) • Poor software management (BNJ43; DVD-2n37; DVD-2n 45) • Ineffective virus software tools (DVD-2n 72, (DVD-2n60) *Limitations in Security Measures* • Negligence on password usage (BNJ19, BNJ20, BNJ22, DVD-2n21, DVD-2n24, MON23, BNJ21) • Poor security enforcement

Exploratory Notes: * Interviews were done in CPUT, Cape Town Campus with all participants in October/November 2010

Table 11 : Security Aspect on CPUT Systems – CTS Administrator/Technician Perspective

Participants	What are the existing security awareness programs, rules & procedures	What are the existing Security Threats and hindrances	What are the current security Measures	Explanations
Network administrator	• Educate users through induction (OF_NET48, OF_NET466)	• There is always security breach (OF_NET63) • Denial of service (OF_NET14) • Poor network functionality (OF_NET56) • Numerous viruses and worms (OF_NET4)	• Use of McAfee or AVG antiviruses (OF_NET9) with sniffing tools (OF_NET18) and firewalls (OF_NET26) that are updated almost every day (OF_NET12). • Access to the system is limited to registered students only (OF_NET23) • However, user account password should be designed to be 8 characters and more (OF_NET38).	*Security Awareness Programs:* • General workshops for new people (OF_NET466) *Existing Threats:* • Mainly denial of service (OF_NET14) • Malfunction of network (OF_NET56), mostly due to number of viruses and worms (OF_NET56) *Security Measures:* • 2 different anti-virus software applications used, with sniffing security tools, and firewalls (OF_NET9, OF_NET18, OF_NET26) • Only legitimate users have access to the system (OF_NET23) • Desired proposed password criteria should be 8 characters

Exploratory Notes: * Interviews were done in CPUT, Cape Town Campus with all participants in October/November 2010

4.2 User Perspectives on the Security Aspects of e-Learning

Discussions about the status of security aspect in e-Learning systems (CPUT Case) on the study are drawn from Table 9 (Academic Experiences), Table 10 (Students Experiences), and Table 11 (CTS Administrator/Technician Perspective). According to chapter four of this thesis, the Work-Activity Framework presents the e-Learning process as an activity system. An activity system according to Hardman (2005:381) is made up of interrelated components such as actors, who carry out specific but interrelated activities to achieve clear goals.

The outcome of the activities however, is dependent on various mediating factors (mediators). For the purposes of this study, the key actors in the security process of an e-Learning system in a higher education institution are academics, students and network administrators. Findings on the perspectives of academics are discussed in Table 9, followed by students' perspectives in Table 10 and of CTS administrators/technician in Table 11. Each table is discussed in detail in sections 4.2.1 – 4.2.3.

4.2.1. Educator Reflections on e-Learning Security

This section summarizes the teacher responses based on the main research questions in Chapter one. As indicated on the Work-Activity Framework, academics use the LMS to control the learning content and to facilitate learning. The assumption in this statement is that academics should have a certain level of knowledge about the LMS and its features if they are to use it effectively. Awareness of the security aspects of using an LMS as well as a conducive environment for the implementation of security solutions in an e-Learning environment are even more important in ensuring a safe and productive use of the systems in educational processes. However, findings reveal a less than convincing level of knowledge about the LMS, its security aspects and the adequacy of existing security measures, among CPUT academics.

A departmental investigation reveals that many lecturers are not even using the existing e-Learning platform, Blackboard (In a conversation on 25 March 2009 Pin_IT; and 27 March 2009 Tmak_IT); nor do they have understanding of security capabilities the platform offers to assessment processes (In a conversation on 27 March 2009 Mak_IT; 24 March 2009 Har_IT). The literature has shown the number of benefits that e-Learning systems offer to help teachers in their teaching; thus the department would benefit if staff could get to utilize the platform fully for its teaching and assessment processes. What has emerged frequently from

departmental interactions is the lack of understanding that exists, not only of the e-Learning system but also of concerns on how safe it is to use for assessments

In terms of limited knowledge, academics complain of a lack of training on LMS usage. On this point for example, one lecturer said that they adopted the LMS to enhance their teaching even though they were never given instruction on how to use it effectively (MM_IT10). As a result, several lecturers are uncertain about the potential capabilities of an LMS. For example, one lecturer was not even sure if an LMS could handle all data types (MN_IT43). Another lecturer could only assume that an LMS should be able to handle various types of data, without necessarily knowing which formats could and could not be handled by this system (MM_IT22). It is not surprising therefore, that some of the lecturers are not exploiting the communication features offered by an LMS, but prefer to use their personal emails (CST_IT75, MB_PR46). In effect, a large number of educators were not using the LMS for educational purposes. In addition to limited knowledge about the uses of the system, technical failures were outlined as a major hindrance to system usage. In explaining this problem, one lecturer went as far as to say "you can't do anything and students can't submit assignments ..."(RT_IT14), meaning that despite the intention, there are times when it is often just technically impossible to use the system.

Factors such as a lack of security guide lines, poor computer and network functionality, and slow or constant denial of service, were also cited as additional sources of frustration and hindrances to LMS usage at CPUT. For those who want to use the system, poor security aspects often compromise efficiency and the security of academic processes. In explaining this level of frustration, one lecturer said "we schedule a test and then we have to postpone because of the system or the internet that is not working" (Mak-IT7).

A list of security threats cited was very long, ranging from tool usability failures, slow computers or unstable network related problems to disruptive pop-up messages (CST_IT73; Mak-IT39; Mak-IT54; MB_PR30; MB_PR29; CST-52). A slow network in particular, is described as a hopeless situation, and a major irritation. Another lecturer for example, complained that the LMS is hopelessly unstable and slow; as a result, she does not trust it for assessments at all (CST_IR73). Other lecturers are using very noisy and old computers that often freeze (Mak-IT54; MB_PR25), often due to a poor network that is congested with viruses and worms (MB_PR29; Mak-IT53; PR_TND99; CST_IT52). These conditions make it almost impossible for the academics to efficiently use the system for quality teaching purposes.

Academics claimed that they were reluctant to report these problems because of the time it takes for the problems to be solved.

In terms of the basic practices, not all security measures are enforced all the time. Academics reported that they had never changed the login details to the LMS. Some lecturers indicated that they are still using the same security login details that they used when they started using the LMS (CST_IT17, MB_PR4). In addition, they are currently having passwords with the minimum of six numbers or characters only; there was no instruction to them to use any specific password criteria. In terms of pro-active security measures, most lecturers believe that the CPUT anti-virus software should be up-to-date, even though they do not even know whether or not is updated regularly. As a result some of the academics do not even know how to update the anti-virus software, let alone having it installed on their work computers. These negative experiences of academics about the LMS are obviously encountered by students as well.

4.2.2. Students' Reflections on e-Learning Security

Students are equally affected by security limitations in the e-Learning systems at CPUT. According to the findings on students' experiences, security hindrances varied from limited (denied) access to the LMS, inadequate skill on how to use the LMS, poor LMS functionality, lack of guiding security procedures, to poor resource or network functionality.

In terms of limited access to the LMS, students feel they are not able to use it as much as they would like, not only due to technical limitations, but also because of poor security practices. For example, students are often disconnected from the system network, and therefore cannot access the learning material or cannot have access to the system at all, due to misappropriation of system-identity (authentication) data. For example, the sharing of security login details with those who did not have access, resulted in log-in failures for some of the students (DVD-2n39; MON49). The students involved wrote emails to their respective lecturers indicating their true identity and explaining that they had used their peer account to access and submit on the LMS (ibid).

Security related technical failures are also a major point of frustration. In most instances, LMS access is denied to everyone – for more than a week, or students do not have any subjects on their LMS page, even though they are registered (MON75; MON120). In terms of explanations, limited skills are cited as the factors that lead to wrong actions which in turn, led

to connection discontinuity. Some students admit that they have never worked on e-Learning systems before, have never been trained, and thus, find it difficult to interact with the LMS (MON114). Even though, students are supposed to use the LMS for their learning, some of them said that they did not know how to interact with an LMS. In this instance, some students claimed that they knew nothing about the LMS (MON116; ABO31), struggled to use it (MON114) or took time to adjust to using the LMS (MON145, MON119). However, students feel that this is caused by a lack of training (BNJ91, BNJ85). Students think that this problem is equally applicable to academics. Assumptions are that some academics are also not familiar with the LMS features that they use in teaching (MON123; MON131).

Even for those who are fairly technically literate, there are system usability complaints, with claims that the LMS interface is not user-friendly and unexciting (MON109; MON110). The concern for students is that they will end up missing significant deadlines when they cannot upload assignments in time, and that they will even lose marks, due to system failures (BNJ4; DVD-2n27; DVD-2n26). It was reported that incompatible software is used in the system, and the tools at the disposal of students were also cited as a frequent obstacle. In this case, students complain that application software incompatibility has led to them, in certain instances, failing to download or upload assignments due on the LMS (BNJ43; DVD-2n37; DVD-2n45). For example, when students submit their assignments on the LMS, the receivers would get them in a corrupted form (DVD-2n 39). When asked to explain the causes of these security related hindrances, a lack of training was given as the key factor. In their account, students feel they have not been introduced to any system security guiding policies or rules (DVD-2n183; ABO35; DVD-2n184; MON150) or attended any introductory training about the security aspect of the system (DVD-2n108; BNJ125; MON154; MON155; MON156 MON157; MON158).

A common assumption among students is that they were somehow ignored when an induction to adequate security practices on the system was given. Because of this lack of understanding of the security practices, they are convinced that security passwords are not supposed to be changed on the LMS (BNJ25; MON30; BNJ26) – and many of them are still using the password that was given to them when they registered (MON29; MON28; MON32). Those passwords are a minimum of six numbers only (BNJ19; BNJ20; BNJ22; DVD-2n21; DVD-2n24; MON23; BNJ21), which is a limited level of security strength. This situation suggests that the presence of a detailed security policy that has effective password criteria with a set minimum level of complexity would minimize the chances of poor security practices on LMSs.

For example, a strong password should have a minimum of eight characters - with a mixture of numbers (0-9), upper and lower case letters of the alphabet, and the symbols found on a keyboard (Kouziri, 2008). A strong password with a combination of these aspects at the very minimum should be recommenced for LMS users to lower the overall risks of security breaches.

Lastly, students mentioned a poor resource or network functionality that persistently denied service as a limiting factor on LMS usage. In their experiences, systems constantly fail due to hopelessly slow computer networks that are infected with multiple viruses and are loaded with obstructive pop-up messages (DVD-2n29; DVD-2n32; DVD-2n60; DVD-2n72; DVD-2n87; DVD-2n90; DVD-2n112; DVD-2n118; DVD-2n222; DVD-2n223; DVD-2n205). Clearly, the fact that the institution provides such technology facilities indicates a willingness to offer technology solutions to its community of users. However functionally will become less than useful, unless the facilities are fit-for-purpose,

The current state of affairs is a concern not only for students, but for anyone who needs to use the system. Understanding the reasons for security shortfalls in the LMS networks at CPUT therefore, is critical if there is to be any hope for the problem to be resolved. With the aim of understanding these reasons, the findings on experiences and the conditions of CTS departmental head/technicians responsible for system maintenance are outlined in section 4.2.3.

4.2.3. Administrators' Reflections on Institutional Network Security

CTS department was formed after a merger between the Peninsula Technikon and Cape Technikons to form the Cape Peninsula University of Technology (CPUT) in 2005. It was only after then that computer services and network administrative units from different institutions (with different working culture and traditions) had to start working together as one department: Computer and Telecommunication Services (CTS). Seven years later (2012), the department is still on its re-design stages to consolidate its operations. In the process, merger challenges continue to affect the quality of computer and network services, including the security of systems.

In contrast to the academics and students who use the system, CTS administrators and technicians are supposed to ensure optimum functionality of networks, and a high quality of service for all the network users (OF_NET21, OF_NET30). Because two institutions merged,

the functions of the network administration department at CPUT are still in a state of change. This means that the administrators are still experiencing operational challenges in ensuring optimum service levels to network users (OF_NET61). The Computer and Telecommunication Services (CTS) which was born of a merger of the IT and Network departments in 2005 (OF_NET26), had to reconcile operational complexities such as re-defining job-descriptions, staffing, the work culture and infrastructure consolidation of its merging units. For example, whilst the IT department specialized in computer hardware and software related services, the network department mostly rendered networking services to network users (ZN_1).

Everyone was used to the job-descriptions and working conditions they had been working under, for a number of years, meaning that tasks and operational boundaries were clear and simpler. However, after the CPUT merger, the CTS department offered various services to clients, ranging from the maintenance and support of integrated academic and administrative systems, printing, email, networking (including intra and internetworks), directory services, Novel platform support, desktop management, to security services and access controls (to electronic and non-electronic facilities). The mixture of new functions within one department meant that each technician had to learn an additional function in a newly formed department. One technician for example, reports that there were two unstable network links in the Wellington campus, where they had to trace the problem with the links (OF_NET18; ZN_13). Unit merger also brought changes in management, which called for adjustments to new conditions among the personnel (OF_NET49; ZN_15). Considering personnel, one technician complained "... and at the moment we've got staff shortages" (ZN_14).

Limited capacity in terms of fewer technicians and fewer centers of operation relative to an increased number of campuses, faculties, departments and clients to service per technician – were also cited as explanations for why there were challenges in network services. According the technician at CTS for example, CTS offices are situated in five of the eleven CPUT campuses (OF_NET21; ZN_9). Each of these offices has its own specified operating hours for CPUT students and staff. Students visit the offices for support, whereas staff can log a call on the service desk phone number or email address that is specified in the CTS website. The five campus administrators and technicians are also responsible for providing services to other six campuses, where, in most cases, they often find their capabilities too over-stretched to be effective (OF_NET18; ZN_10; ZN_17). In terms of Apple Mac support for example, as of 2012 only one technician is servicing all the Apple Mac users in the eleven campuses (ZN_22).

CTS is also responsible for the administration, maintenance and servicing of sundry electronic services such as telephony, backups, online personal application (OPA) for academics and students. The list of responsibilities also includes e-Learning hosting, help-desk service, video conferencing, library support, IT Centre, bulk sms, audit support, registration, cross-functional and administration as well as service management. Even though the department is offering this wide range of services to users, there is instability in some of the services. The following are listed as the problem systems "email, the internal computer network, the wireless links connecting the remote sites to the two main campuses, Blackboard (WebCT) server, OPA services and the Mowbray wireless instability" (Ten-2012; ZN_1; ZN_4). In order to maintain improvements to the services, the department is conducting a project to stabilize major systems.

This study aimed to understand how existing network and security programs for users are communicated and practiced, what the security vulnerabilities in the e-Learning platform are, and the ways to reduce those threats. The researcher interviewed a representative from the CTS department in the Bellville campus in order to broadly understand the extent to which the security problems encountered in the network directly affect the teaching and learning services. When asked if the department expected to communicate expected security guidelines, network rules and procedures to users. The network representative responded that they attempt to communicate through an induction process (OF_NET48). The induction process only takes place in the beginning of each academic year. Unfortunately it does not guarantee that it will have a good student attendance.

As a result, the representative contends that even though "network security procedures are communicated", they are not properly practiced by users because there are loopholes in security of the system (OF_NET63). He further indicated that clearly there are users who sometimes breach security rules and policies of the systems. For example, the CTS departmental head has mentioned that the most common hindrances affecting the network are the denial of service, and a very slow network full of viruses and worms (OF_NET4; OF_NET56). All these afore-mentioned security and network performance threats contribute to a poorly functioning system and an unacceptable standard of the service. These hindrances are evidence of how untrusted, unstable and unreliable is the CPUT system is, that is used for teaching and learning. In order to put into practice good security measures, the department uses two different anti-virus programs to help reduce poor service delivery. At the same time, they use firewalls and sometimes a sniffer as protecting security measures.

Now starting the findings on the security aspect of e-Learning from a Work-Activity Framework perspective are outlined in detail in section 4.3.

4.3 Findings on e-Learning Security at CPUT

The starting point in this study was to ascertain the reality of the security threats in the e-Learning environment, processes and practices at CPUT. As described by (Weippl & Ebner, 2008), security is essential, it is meant to protect against a risk or a threat. However, the findings revealed that the LMS at CPUT are continuously exposed to security threats that negatively affect performance, and have now become a venue for illegal activities. In this study, security threats are referred to as a potential risk that harms the system and further causes vulnerability of the CPUT e-Learning environment. However, details about security threats are discussed in the section below, and a larger part of the findings outline the causes of and give explanations about the present situation.

Thus, drawing on the work activity framework for security analysis in e-Learning system in Figure 4, the following key concepts are used to present findings on the security aspect of e-Learning. According to the framework, success or failure of the security aspect of e-Learning is dependent on the interplay between the goals of various actors in an e-Learning environment, and a synergy between activities and their mediating factors. In other words, a secure e-Learning environment is mediated (facilitated and made possible) by:

- Adequacy of security awareness programmes in the institution
- Relevance of existing security measures
- Consistent adherence to sound security practices (by administrators and users)

4.3.1 Adequacy of Security Awareness Programmes

The activity theory framework in Figure 4 presents the security aspect of e-learning as the activity system that consist of various but related components including actors, their goals, mediating factors (mediators), activities and outcomes, as well as tensions between mediators, actors and activities. Mediators refer to the factors that enable as well as those that can hinder activities and the realization of a positive outcome. One of the main mediators of adequate security is awareness, which in turn requires awareness programmes to be in place and to be successfully implemented, by CTS administrators, as coordinators, and the rest of system users (including educators and learners).

Whilst the actual security tools are of paramount importance, implementation of these tools becomes impossible without awareness. Thus, the emphasis in the framework is that satisfactory security awareness programmes for users should be a priority. It should be a major part of the entire internetwork planning, design, and implementation processes within CPUT. Security awareness programmes in this study represent orientation workshops, guiding rules, policies, procedures and compliance systems to guard the LMS platform at CPUT. A lack of awareness programmes, according to the activity theory framework therefore, is likely to be accompanied by a lack of user awareness and, ultimately, a lack of security implementation in the institution.

The presence of security programmes on the other hand, is a significant mediator of security practices in the e-Learning security activity system. However, according to the framework in Figure 4, the presence of this mediator alone will not be adequate. It is also necessary that all stakeholders have awareness of this including administrators, courseware developers, educators and learners. Clearly, as impressive as the presence of the latest security features, applications and procedures are, it is of no use if they are not being implemented simply because no one is aware of them or the purpose and procedures of their implementation.

Findings indicate that only very minimal security awareness programmes on e-Learning platforms exist at CPUT. In fact, students and academics were not even aware of any guiding security programs, rules and procedures. A lack of introductory training initiatives for first time network users in particular, was cited as a major concern. As a result, the level of awareness and literacy on e-Learning security practices was found to be extremely minimal among system users, such as educators and learners. There is also a need for a continuous workshops and related training sessions for all systems users at CPUT.

Given the clear coherence between the framework guidelines Figure 4, that a lack of awareness programmes is likely to lead to a lack of security implementation, and then it is not surprising that the apparent lack of security in the findings is then followed by unsound security practices in the IT Networks and the e-Learning environment. Hence, it is only logical to recommend the strengthening not only of awareness programmes, but also their implementation at CPUT.

Thus, the relevance of existing security programmes and related awareness measures becomes even more significant.

4.3.2 Relevance of Existing Security Measures

Whilst the presence of security tools and security awareness programmes, are a significant mediating factor in the e-Learning security framework in Figure 4 – the same framework further emphasizes the relevance of such awareness programmes to the practical security needs of system users. In other words, there is no point in boasting about having anti-Virus software in every work-station if the software is outdated and weaker than the latest threats into the system (Apampa, et al., 2008). It would also be inadequate for mobile network users to focus only on anti-virus software and ignore measures against possible network breaches and intrusions (Mlitwa & Birch, 2008).

Whilst security measures against known and unknown threats exist, findings revealed security loopholes within the CPUT networked systems. Network users claim to work on very slow and annoying computers connected to a mostly non-responsive network that often ends up delivering corrupt information to recipients. To account for this situation, the CTS department cites a continued imbalance between the two different sets of security measures inherited from the old Peninsula and Cape Technikons, which were combined after the merger, and are yet to be fully consolidated. According the analytical framework Figure 4, a lack of relevant programmes will be a handicap to the implementation of security practices in the e-Learning environment. The lack of quality and relevance of the existing security measures is equally associated with poor security practices at CPUT. On this basis then, drawing from the assumptions of a theoretical framework, it is considered useful to make recommendations.

It is recommended therefore, that users should be trained to properly use appropriate available security measures and to be frequently reminded that they must take the best possible security precautions, such as changing passwords frequently. Similarly CTS administrators and technicians should frequently maintain and update networked systems to improve network performance and to ensure the adequacy of available security practices.

4.3.3 Adherence to Sound Security Practices

In addition to the adequacy and relevance factors, the framework Figure 4 also emphasizes the actual implementation as one of the enabling mediators, with consistent adherence to sound security practices as a critical component. Obviously, the value of security tools and applications can only be appreciated if implemented correctly, hence the emphasis on adherence to sound practices (Slay & Koronios, 2006:178). Adherence to sound security

practices according to the analytical framework Figure 4 implies that information stored on safe and secure learning tool gets delivered to the intended recipient securely and efficiently. In this ideal situation, network users are identified by the LMS through the authentic use of strong passwords and usernames. Of course, passwords are changed regularly, so as to maintain the security of the system. LMS users also access uncorrupted material from the network. Similarly, the network is protected from any harmful attacks that could interrupt teaching and learning processes.

Without these enablers, the framework Figure 4 predicts a limited or complete lack of adherence to security practices in e-Learning programs. According to the findings, a lack of authentic user identification, poor LMS and network functionality in the e-Learning environment is equally associated with poor adherence to sound security practices in e-Learning system at CPUT.

4.4 Conclusion

In this chapter, the findings, a discussion and explanations are presented in detail. In this discussion, security measures, tools and processes are confirmed to be inadequate. The security measures in the e-Learning environment in the institution are inadequate, as is the awareness about the necessary security measures among students and academics. Although training programmes on sound security practices exists, lecturers and students seem to be unaware of them and complain about the lack of training that is available. Along with this shortfall is poor adherence to security measures by these system users. Even the minimal security measures that exist are not being fully implemented by network administrators.

A research problem was that, the security aspect in e-Learning systems has gained minimal attention, leading to poor access and use of the electronic teaching and learning systems at CPUT. The aim of the study was to look at the present situation, to look at the causes, to listen to explanations, and ultimately, to build some insight that would lead a researcher towards solutions. The conclusion in this respect is that systems security measures are poor. This has a direct co-relationship with system failures and limited usage. Insight from the activity theory framework points to a gap between the goals of e-learning and the mediating factors towards a secured e-Learning environment in the institution. Therefore, insight is drawn from the framework Figure 4 and the literature conclude and to present recommendations in chapter five.

CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS

5. Introduction

The previous chapter presented research findings based on the overall objectives of the thesis. However, this chapter provides an overview of the findings, discussing whether or not study objectives have been met, with a conclusion, recommendations and possible areas for further research. The study further uses the Work-Activity analytic framework to inform the conceptualized e-Learning security framework based on the empirical findings, and the subsequent recommendations. Thus, the chapter opens with a summary of findings with recommendations for each problematic item in. This is followed by a detailed explanation of recommendations in section 5.2. Limitations of the study as well as suggestions for further research are presented in sections 5.3 and 5.4 respectively.

Table 12: Summary of Research Findings

Research Objective (A,B,C)	Academics			Students			IT/Network Administrators		
	Summary of Findings	Explanation	Recommendations	Summary of Findings	Explanation	Recommendations	Summary of Findings	Explanation	Recommendations
Understand LMS & security awareness programmes (A)	• Very limited security awareness : ranges from none to minimal awareness	• Lack of introductory training programmes • No precise awareness programmes	• All support divisions to integrate security element into all programmes of operation • Establish & enforce continuous security awareness programmes	• Poor level of awareness, ranging from none to minimal awareness	• Lack of introductory training • No specific awareness programmes	• All support divisions to integrate security element into all programmes of operation • Establish & enforce continuous security awareness programmes	• Adequate awareness is evident, but implementation of the known is inconsistent	• Technicians specialize in secure practices. • There' are adequate awareness programmes	• Monthly training on network security for all users. • Also set clear responsibilities to conduct security programmes, with accountability roles & time lines.
Identify existing security threats (B)	• Multiple network attacks ranging from viruses, pop-up messages, Denial of service (DoS) • Regular system failure • Limited LMS knowledge	• Poor security measures • Negligence • Ignorance on password criteria & usage • Lack of LMS/network skill • Limited bandwidth, leading to lengthy response delays	• Pro-actively (rather than re-actively) strengthen security programmes • Renew focus on consistent adherence to sound procedures both for the general network, & for the LMS environment. • Training of sound security measures for academics must be enforced • Instead of auto reminders, software auto updates must be implemented to ensure upgrades.	• Multiple attacks on network : viruses, pop up messages, Denial of service (DoS) • Limited knowledge about LMS • Regular system failure	• Negligence & inadequate security measures • Ignorance on password criteria & usage • Lack of skill • Lengthy response time leading to regular LMS & system failure	• Pro-actively (rather than re-actively) strengthen security programmes • Renew focus on consistent adherence to sound procedures both for the general network, & for the LMS environment. • Training of sound security measures for students must be enforced • Instead of auto reminders, software auto updates must be implemented to ensure upgrades.	• Multiple attacks on network : viruses, pop up messages, Denial of service (DoS) • Regular system failure	• Imbalance of current security measures • Staff shortage following restructuring during university merger	• Frequent update of existing technology with latest innovations • HR to recruit more skilled technicians to address staff shortage. • Set clear responsibilities to conduct security programmes, with accountability roles & time lines. • Clear interaction between support divisions & users (learners & academics).
Security measures & the extent of their implementation (C)	• Security guidelines unknown • Use outdated security precautions • Incompatible hardware & software • Inadequate implementation of security measures	• Lack of clear network security policies & guidelines • Poor enforcement of security measures • Lack of guidance • Use of old devices	• Implement security guidelines • Enforce security compliance mechanism for all network users • Monitor, review, evaluate security measures • Provide guidance & support to users • Provide latest devices & technology	• Security guidelines unknown • Use outdated security precautions • Incompatible hardware & software • Inadequate implementation of security measures	• Lack of clear network security policies & guidelines • Poor enforcement of security measures • Lack of guidance • Use of old devices	• Implement security guidelines • Enforce security compliance mechanism for all network users • Monitor, review, evaluate security precautions • Provide thorough guidance & support to users • Provide latest devices & technology	• Ineffective available security measures • Imbalance of security measures • Incompatible hardware & software	• Poor adherence to available security measures • Poor implementation of security measures due to university merger • Staff shortage following restructuring during merger	• Implement security guidelines • Enforce security compliance mechanism for all network users • Monitor, review, evaluate security precautions • Provide guidance & support to users • Provide latest devices & technology • Recruit more staff

Table 12 presents a summary of research findings for academics, students and IT/Network department staff based on the research problems. The table shows the summary of research findings with their explanations and recommendations for each participant. The content of table, with emphasis on recommendations, is discussed in detail in the following section.

5.1 Recommendations

Three key aspects of security in e-Learning platforms stand out in the summary of findings in Table 12. These are:

- Availability (and quality) of security awareness programmes;
- The reality of security threats within the institution, as well as
- Availability (and quality) of security measures (including the extent of implementation).

5.1.1 Availability of Security Awareness Programmes

The work activity framework in Figure 4 suggests that a security environment on e-Learning platforms is dependent on specific mediating factors. An ideal environment with related practices for example, depends on the presence of, and a positive co-relationship between the goals of the actors, the mediating factors, activities and outcome/s. The framework outlines the following key mediators: security awareness, effective security measures, bandwidth, adequate skills, and networked computers with an LMS platform, clear security policy and guidelines as well as the strict enforcement of preferred security solutions. The presence of these mediators and a supporting linkage between them and the goals, tools and activities is considered to enable (mediate) an effective and a secure e-Learning environment. In the absence of, or limitations in, this order – the converse is also assumed in the framework.

On the security awareness mediator, a discrepancy is evident in the findings, regardless of the fact that the presence of multiple security threats is well known among users and service providers. Given the absence of the awareness mediator according to the framework, a negative outcome can be anticipated. In fact, a lack of security awareness programmes among system users (educators and learners) is also associated with poor security practices in the e-Learning environment at CPUT. For this reason, drawing on the framework to provide insight, in order to make recommendations, becomes logical.

5.1.1.1 Recommendations on the Awareness Programmes

The problem of poor awareness by academics and students is linked to the shortage of security awareness training and campaigns. Therefore, it is recommended that the CTS department should incorporate the security aspect into all its areas of operation. However, the CTS department should first set clear roles and responsibilities for their own personnel. Officials must allocate specific responsibilities to respective administrators, with enforceable personnel roles of accountability, to conduct awareness campaigns for academics and students on a regular basis. The department should write and keep up-to-date a clear network policy, IT tools and network usage guidelines, and enforce user attendance at their training sessions. In this case, the department should have liaison with the heads of all academic departments to generate a random list of staff who will be attending trainings on a weekly basis. The IT department should also work together with the e-Learning department, ensuring that e-Learning administrators and all e-Learning systems users are involved in transformed practices.

As a key stakeholder in the security work-activity framework Figure 4, the e-Learning department should also play a major transforming role. It should nominate administrators who will conduct awareness training sessions that introduce users to best security practices.

Findings also reveal a lack of awareness about existing security measures and sound practices among academics. As hosts of major actors in the security work-activity framework (the academics), academic departments should work much closer with both the IT and e-Learning departments in consolidating a secure e-Learning environment in their practices. Academic departments should invite e-Learning and network administrators to conduct monthly workshops about security awareness and new trends.

Curriculum officers within academic departments should work with the e-Learning and network administrators to ensure that appropriate training exists. Equally important are teachers and students within their academic departments who should attend trainings in order to acquire adequate skills. It is therefore appropriate to explore the application of security measures to minimize the existence of current security vulnerabilities.

5.1.2 Availability of Security Measures

The availability and extent of security measure usage are equally important in this thesis. However, unclear security guidelines, the use of old infrastructure, minimal user knowledge, and minimal implementation and security measures are also outlined as a major concern. As a recommendation, the CTS department should thoroughly formulate a network policy that will address implementation and security guidelines on the network. The network department should be constantly reviewing, monitoring, and evaluating the practice of security precautions – and make the document easily accessible for both academics and students.

Further, the Computer and Telecommunication Services (CTS) department should provide adequate and compatible network infrastructure with the latest image. The department should also work hand in hand with the departmental technicians. Enforcement of security compliance mechanisms that will enforce users to practice good security applications should be prioritized. In essence, when a security feature or condition has been highly considered at CPUT, it would make a positive contribution to the quality learning through the use of the LMS. Nonetheless, it would be particularly beneficial to also recommend similar studies to adopt the work-activity framework as an empowering tool.

5.1.3 Neutralizing the Severity of Security Threats

Regular virus attacks of networks, leading to a frequent denial of service are a major hindrance to the use of the network and the LMS. This situation is mostly caused by the staff shortage, minimal implementation of active security measures, inappropriate application of security measures and major weaknesses in passwords' criteria. To improve this situation, it is recommended that the human resources department should recruit more skilled technicians and administrators to ease the workload and address the staff shortage within the CTS department. The CTS department should also train both academics and students on how to effectively use the LMS security measures. Network users and the administrators should improve their interactions - to improve the usage and implementation of resource security measures. Further, the CTS department should pay a closer look at the maintenance of existing infrastructure and keep it maintained to a high standard.

Similarly, the CTS department should have a tool that will not only remind all network users to change their passwords on a bi-monthly basis, but also to insist on a strong password combination. Departmental technicians should also enforce the implementation of adequate

security measures and proper password usage. Both academics and students need to have a thorough knowledge and understanding of the security measures, their application and practice. In the same way, the CTS department should introduce and enforce an auto update of security measures in all networked computers. With all these points, it is therefore appropriate to explore the use and availability of current security measures against threats that leave the learning environment open and vulnerable. Research limitations are outlined in section 5.2.

5.2 Research Limitations

Even though the study has been successfully conducted to achieve the intended goals, and has recommendations and suggestions to bring insight to bring to the shortfalls encountered in the security systems. It did encounter a few limitations. For example, this thesis did not focus on other universities in other provinces that use LMS to enhance their teaching and learning. This was due to time constraints. More research and investigation could be conducted on this area to reach a general conclusion, since this study focused on CPUT only. In addition, some planned interviews could not be conducted due to the busy schedules of teachers and technicians. The few who were cooperative could only spare a few minutes of their busy working time.

Suggestions for further research brought forth by this study are set out in section 5.3.

5.3 Concluding Remarks

The objective of this study was to understand the extent to which security measures on e-Learning practices are implemented at CPUT. This work-activity framework on Figure 4 was then used as an analytical tool towards this end. In essence, the framework has helped the researcher to better understand, conceptualize and interpret the security aspects of e-Learning as a shared activity system with different participants (actors). Within an activity system, actors aim to achieve their intended goals – join together by a common objective through activities carried out in the system. Secure e-Learning activities however, depend largely on the positive interplay between actors, the mediating (enabling) factors and respective activities of each actor in a system. In a sense, a mediator will either facilitate or inhibit the outcome, depending on whether it is present; it is in an enabling condition and whether it has a stronger impact than the tensions between stakeholders and processes in the activity system. In this respect, the work-activity analytic framework was useful in outlining the state of mediators, the tensions in the process, the severity of problems and loopholes within the e-Learning systems, to the extent of simplifying the process of making recommendations.

Findings revealed a poor security measures throughout the networks and the e-Learning environment at CPUT, mostly because of inadequate tools and loopholes in implementation processes. In this respect, the framework was used as a basis for the following recommendations:

- On the lack of security training programmes due to unclear provisions, guidelines and commitment by related officials: Strengthening the quality, relevance and frequency of training programmes and clarifying roles and responsibilities for staff to conduct these, is recommended.
- On user security-awareness, this is linked to unclear network usage guidelines and poor participation to training sessions by staff. Clear reviewed, monitored and effective implementation of network guidelines: more involvement of academic departmental heads and other departments in insisting on staff participation in training workshops is recommended.
- On adherence to security measures, this is lacking due to minimal guidance and policy enforcement: - Clear security policy with effective usage of security measures, and adequate user guidelines are recommended.
- On the poor network and LMS functionality which is linked to the existence of multiple threats: -, the taking of sound security precautions by the CTS department to ensure improved performance and implementation of safety provisions is recommend
- On the imbalance of the existing security measures relative to the existing threats: - A set of strong password criteria, the availability of latest technology and the use of effective, up-to date antivirus software, together with a clear allocation of tasks and responsibilities by the CTS department is recommended.
- On the lack of implementation of security measure which is linked to poor user compliance and limited usage of protection measures: -, The review of network policy, implementation and enforcement of compliance tool by the CTS department to ensure that all users adhere to the policy is recommend

Lastly it is also suggested that the human resource department should address the issue of the staff shortage within the CTS department to ease the workload.

5.3.1 Suggestions for Further Research

Recommendations for further research are based on the findings, limitations and scope of the study. The sample was limited to data from one university, the Cape Peninsula University of Technology (CPUT) in the Western Cape. Given the urgency of the topic it would be useful to know whether results would be similar if other universities were also included. For this reason, other universities from different provinces should be added in future studies.

IT security is a broad concept that is informed by a variety of interrelations between various stakeholders and practitioners within an institution. The study focused only on the e-Learning systems environment, which is just one of many environments in a broader security component of the electronic environment of the institution. As valuable as the study turns out to be, a more comprehensive investigation into other contexts e.g. security of physical networking devices and encryption - would broaden insight on this subject.

LIST OF REFERENCES

Allan, M.J. 2002. Cultural Borderlands: A case study of cultural dissonance in an international school, *Journal for Research in International Education*, Volume 1, No. 1, pp. 63-90.

Allen, D., Karanasios, S. and Slavova, M. 2011. Working with activity theory : Context, Technology, and Information Behavior, *Journal of the American Society for Information Science and Technology*, 62(4), 776-788.

Angel **see** Angel online http://angel.uwc.ac.za/index.php?module=splashscreen# http://www.sun.ac.za/ekampus/indexe.htm [accessed 19 September 2008]

Apampa, K. M., and Wills, G. B. 2008. Electronic integrity issues in e-assessment security. ICALT 2008: The 8th IEEE *International Conference on Advanced Learning Technologies*, Spain.

Apampa,K.M., Wills, G. and Argles, D. 2008 Towards Security Requirements in Online Summative Assessments, School of Electronics and Computer Science, University of Southampton, UK.

Arth, B. 2011. The Business Impact of Next-Generation e-Learning, How Today's e-Learning Drives, Business Results, Bersin and associates research report Volume 1.0.

Assefa, S. 2009. An Information Security framework for e-Learning management systems, Master's dissertation in the computer Science, Faculty of science, University of Johannesburg.

Babbie, E. and Mouton, J. 2001. The practice of Social Research. Cape Town: Oxford University Press South Africa.

Barbie, E., and Mouton, J., 2004. The Practice of Social Research: South African edition Oxford University Press, Cape Town, South Africa, ISBN 0 19 571854 2.

Baxter P., and Jack, S. 2008. Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers, McMaster University, West Hamilton, Canada The Qualitative Report Volume 13 No. 4 pp. 544-559 http://www.nova.edu/ssss/QR/QR13-4/baxter.pdf. [accessed 2 August 2010]

Beebe, M. 2006. Afghans' Next Generation: eLearning, International Research and Development Washington State University, http://linc.mit.edu/linc2010/proceedings/session1Beebe.pdf [accessed 29 September 2008]

Bennet, A. and Bennet, D. 2008. e-Learning as energetic learning, VINE, Vol. 38 No. 2, pp. 206-220.

Bhattacherjee, A, 2012. "Social Science Research: Principles, Methods, and Practices" Open Access Textbooks. Book 3. http://scholarcommons.usf.edu/oa_textbooks/3. [accessed 04 June 2012].

Blackboard **see** Cape Peninsula University of Technology e-Learning page.

Bless, C. and Smith, C. H. 1995. Fundamentals of social research methods: An African perspective. (2nd edition). Cape Town: Juta.

Boland, R. J., and Lyytinen, K. 2004. "Information Systems Research as Design: Identity, Process, and Narrative," in Information Systems, Research: Relevant Theory and Informed Practice, B. Kaplan, D. Truex, D. Wastell, T. Wood-Harper, and J. I. DeGross (eds.). Boston: Kluwer Academic Publishers, pp. 53-68.

Brennan, J and Shah, T 2003. Report on the implementation of progress files. Centre for Higher Education Research and Information, Milton Keynes, UK. http://oro.open.ac.uk/324/1/ProgressFiles.pdf [accessed on 6 July 2010].

Brooke C. 2002. What does it mean to be 'critical' in IS research? JIT Volume 17, pp.49-57, Faculty of Business and Management, University of Lincoln, Brayford Pool, Lincoln, UK.

Buchem,I., Attwell, G., and Torres, R. 2011. Understanding Personal Learning Environments: Literature review and synthesis through the Activity Theory lens, Beuth University of Applied Sciences Berlin, Germany .

Caeiro, M., Anido, L. Fernandez, M. Santos, J. Rodriguez, J. and Llamas. M., 2002. *Educational metadata and brokerage: Computers and Education*, Volume 38, No.4, pp.351–374.

Cape Peninsula University of technology (CPUT) online 2010.; [viewed on 5 July 2010], e-classroom http://eclassroom.cput.ac.za/webct/entryPageIns.dowebct

Carliner, S. 2005. Commentary: Assessing the current status of electronic portfolios. *Canadian Journal of Learning and Technology*. Volume 31, No. 3, pp.121-132.

Carliner, S. 2005. Integrating the web into education for technical communication majors: A process-oriented approach in Day, M. and Lipson, C. *Technical communications and the world wide web*. Mahwah, New Jersey: Lawrence Erlbaum Associates pp. 263-284.

Carr, T., and Czerniewicz L., 2007. *International Journal of Education and Development using Information and Communication Technology* (IJEDICT), 2007, Vol. 3, No. 4, pp. 2-6. Editorial: Emergent Research from Southern Africa University of Cape Town, South Africa.

Charmaz, K 2006. Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis, 1st edn, Introducing Qualitative Methods, SAGE Publications, London.

Clark, R. C., and Mayer, R. E. 2003. e-Learning and the Science of Instruction: Proven Guidelines for Consumers and Designers of Multimedia Learning. San Francisco: Jossey-Bass.

Clark, Y. and Toto, R. 2006. Mentoring students online. Retrieved from the World Wide Web: www.tlt.psu.edu/suggestions/mentor. [Accessed on 7 February 2011].

Cole, M. and Engeström, Y. 1993. A cultural-historical approach to distributed cognition, in: G. Salomon (Eds.), Distributed cognitions, psychological and educational considerations (pp. 1-46). Cambridge: Cambridge University Press.

Creswell, J.W., 1994. Research design: Qualitative and quantitative approaches. Thousand Oaks, CA: Sage.

Creswell, J.W., 2008. Educational research: Planning, conducting, and evaluating quantitative and qualitative research. Upper Saddle River, NJ: Pearson/Merrill Education.

Crotty, M. 1998. The Foundations of Social Research: Meaning and Perspective in The Research Process, Allen an Unwin, St Leonards.

Czerniewicz, L., 2008. Distinguishing the Field of Educational Technology. , *Electronic Journal of e-Learning* Volume 6, No. 3, pp.171–178.

Czerniewicz, L.,Ravjee, N., and Mlitwa, N., 2006. ICTs and the South African Higher Education: Mapping the Landscape. Higher Education Monitor, No. 5, ISBN 1-919856-55-2

Denzin, N. K., and Lincoln, Y. 2005. The Sage Handbook of Qualitative Research (Third ed.), California: Sage Publication.

Dietinger, T. 2003, Aspects of E-learning environments. Graz University of Technology. Retrieved 27 May, 2008, from http://www.iicm.edu/thesis/tdieting_diss.doc

Engeström, Y. 1987. Learning by expanding; Helsinki: Orientakonsultit. In Mlitwa, N.W.B. 2011. Integration of e-Learning System into Academic Programmes in Modern Universities: A South African Perspective. Cape Town: TVK e-INNOVATIONS.

Engeström, Y. 199). Developmental studies of work as a testbench of activity theory: The case of primary care medical practice. In S. Chaiklin & J. Lave (Eds.), Understanding practice: Perspectives on activity and context pp. 64-103. Cambridge: Cambridge University Press.

Eom, S.B., Wen, H.J. and Ashill, N. 2006. The determinants of student's perceived learning outcome and satisfaction in University online education: An empirical investigation. Decision Sciences *journal of Innovative Education*, Volume 4, No.20, 215-35.

Feldstein, M., 2002. What Is "Usable" e-Learning?, ACM eLearn Magazine.

Friedman, K., 2003. Theory construction in design research: Criteria: Approaches, and methods, Department of Organisation and Leadership, Norwegian School of Management, Oslo, Norway.

Gall, K.,D.W. Knight, L.E. Carlson, and J.F. Sullivan. 2003. Making the grade with students: The case for accessibility. *Journal of Engineering Education* Volume 92, No. 4, pp. 337–43.

Georgette, W. 1997. "Beyond Media Globalization: A Look at Cultural Integrity from a Policy Perspective", Telematics and Informatics Volume. 14, No. 4, pp. 309-321.

Gillespie, G. M. 2012. *Guide to advising international students about academic integrity*. Retrieved from http://dus.psu.edu/mentor/2012/03/guide-to-advising-international-students-about-academic-integrity

Govindasamy, T., 2002. Successful implementation of e-Learning Pedagogical considerations, Internet and Higher Education, Volume. 4 pp. 287–299.

Groves, S., and Dale, J. 2004. Using activity theory in researching young children's use of calculators, in AARE 2004 : Doing the public good : positioning educational research ; AARE 2004 International Education Research conference proceedings, *Australian Association for Research in Education*, Melbourne, Vic., pp. 1-11. [accessed 17 May 2012].

Guba, E. and Lincoln, Y. 1994. Competing paradigms in qualitative research. In Denzin, N.K. & Lincoln, Y. S. (eds). *Handbook of qualitative research.* Thousand Oaks, CA: Sage: pp. 105-117.

Gunasekaran, A., McNeil, D.M., and Shaul, D. 2002."E-learning: research and applications", Industrial and Commercial Training, Volume. 34, No. 2, pp. 44 – 53.

Hardman, J. 2005. Activity theory as a framework for understanding teachers' perceptions of computer usage at a primary school level in South Africa, Volume 25, No. 4, pp. 258-265

Hashim, N.H. & Jones, M.L. 2007. Activity Theory: A framework for qualitative analysis.
Hassler, V. 2001. Security Fundamentals for E-Commerce. Computer Security Series. Artech House, higher education institutions – a case of UWC, www.hicte.uwc.ac.za. [accessed on 12 January 2012].

Hayaati, N., Alwi, M., F., and Ip-shing, F.M. 2010. E-*Learning and Information Security Management*, Cranfield University, UK, IJDS, Volume 1, No. 2, pp. 148-156.

Henning, E., Van Rensburg, W. & Smit, B. 2004. Theoretical frameworks. Ch 2 In Henning, E., Van Rensburg, W. & Smit, B. 2004. Finding your way in qualitative research. Van Schaik Publishers: Pretoria.

Hotrum, M. 2005. Breaking Down the LMS Walls, International Review of Research in Open and Distance Learning, ISSN: 1492-3831, Volume 6, No. 1.

Hsieh, H.F., and Shannon, S.E. 2005. Three approaches to qualitative content analysis: Qualitative Health research, Volume 15, No. 9. Pp. 1277-88.

http://www.abdn.ac.uk/accessibility/reports/ALTNs4_abdn.pdf (accessed 7 March, 2011).

Huck, S.W. 2012. Reading statistics and research, sixth edition, Allyn and Bacon publisher. ISBN-13: 978-0-13-217863-1 ISBN-10: 0-13-217863-X.

Huysamen, G.K. 1994. Methodology for the social and behavioural sciences, Sigma press, Pretoria ISBN 1 86812 4681

Ingraham, B. Conole, G., and Cook, J. 2003, 'Learning technology as a community of practice', Research Strand, Proceedings of ALT-C 2003, 8-10th September, Sheffield.

Jeffels, P. 2005.Usability, the practical approach to accessibility. Online:

Johansen, A.R.A., 2001. Innovation and the post-academic condition.", paper presented at the 2nd Research Conference on University and Society Co-operation (HSS01), Halmstad University, Sweden.

Jung, I. 2000. A Virtual University Trial Project: Its Impact On Higher Education in South Korea. *Innovations in Teaching and Education*, Volume 38, No. 1, pp. 31-41.

Kabay, E.M., 2006. Infosec Update, Msia & Bsia: Division of Business Management, Norwich University. http://www.mekabay.com/courses/industry/iu_wkbk_2006-01.pdf [accessed on January 2012].

Kaplan, B. and Maxwell, J. A. 1994. Qualitative Research Methods for Evaluating Computer information systems. In J. G. Anderson, C. E. Aydin, & S. J. Jay (Eds), Evaluating Health Care Information Systems: Methods and Applications pp. 45–68. Thousand Oaks, CA: Sage.

Kaptelinin, V., 2005. The Object of Activity: Making Sense of the Sense-Maker, Department of Informatics, Umeå University, mind, culture, and activity, Volume 12, No, 1. Pp. 4–18.

Keats, D. 2003. Knowledge environment for Web-based learning (KEWL): an Open source learning management systems suited for the developing world, the technology source.

KEWL **see** Knowledge Environment for Web-based Learning, University of Western Cape

Klein, H.K. and Myers, M.D. 1999. A set of principles for conducting and evaluating Interpretive field studies in Information Systems, MIS Quaterly, Volume 23, No. 1, pp. 67-94.

Korpela, M., Mursu, A., and Soriyan, H., 2002. Information Systems Development as an Activity; Computer Supported Cooperative Work, Volume 11, pp. 111-128.

Korpela, M., Mursu, A., Soriyan, A., Eerola, A., Hakkinen, H. and Toivanen, M, 2004. "IS research and development by activity Analysis and development, Dead Horse or Next wave? " in Kaplan, B., Truex, III, D., Wastell, D., Wood-Harper, AT and DeGross, J.I (eds). Informations Systems Research – relevant supported Cooperative work, 2002 Volume 11, pp. 111-128.

Kourizi E. 2008. Software requirements specifications For KeePass Password Safe Requirements for Version 1.10, Software Engineering, Aristotle University Thessaloniki.

Kutti, K. 1995. Activity theory as a potential framework for human-computer interaction research, Context and consciousness: activity theory and human-computer interactions, MIT, Cambidge, MA.

Labovitz S. and Hardgedom, R. 1981. Introduction to social research third edition ISBN 0-07-035777-8.

Laurillard, D. 2008. Digital technologies and their role in achieving our ambitions for education, Institute of Education, University of London, www.ioe.ac.uk/publications [accessed on 23 February 2012]

Leedy, P.D. and Ormrod, J.E. 2005. Practical Research: Planning and Design, 8th (edn), Pearson, Upper Saddle River.

Leont'ev, A.N. 1978. Activity, Consciousness, and Personality. Englewood Cliffs, NJ: Prentice Hall.

Lokken, F. 2011. Trends in e-Learning: Tracking the impact of e-Learning at community colleges. Retrieved from http://www.itcnetwork.org/images/stories/itcannualsurveymay2011final.pdf.

Lorenzetti, J. P. 2011. Combating online dishonesty with communities of integrity: Promoting academic integrity in online education. Retrieved from http://www.jsums.edu/jsuoaa/resources/Academic%20Integrity%20in%20Online%20Education.pdf.

Marais, E., and Argles, D. 2006. Security Issues Specific to e-Assessments. 8th Annual *Conference on WWW Applications*, 6-8th Bloemfontein.

Miles, M.B. and Huberman, A.M. 1994. Qualitative Data Analysis: An Expanded Sourcebook, 2nd (edn), Sage Publications, Thousand Oaks.

Miller, J. M. 2005, Usability in e-Learning, Learning circuits, http://www.learningcircuits.org/2005/jan2005/miller.htm [accessed on 13 April 2009].

Mjuleni, L. and Mlitwa, N. 2008. Data Security and the emerging 'e-Commerce trends' in the retail industry South Africa. http://dk.cput.ac.za/cgi/viewcontent.cgi?filename=24&article=1004&context=inf_papers&type=additional [7 May 2012].

Mlitwa, N, and Van Belle, J, 2011 "Mediators For Lecturer Perspectives On Learning Management Systems At Universities In The Western Cape, South Africa" PACIS 2011 Proceedings. Paper 135. http://aisel.aisnet.org/pacis2011/135

Mlitwa, N. 2005a. Assessing the adoption and use of ICT for teaching and learning in identities: The ANT Perspective. Paper prepared for the CIRN2006 Conference, Monash University, Prato, Italy.

Mlitwa, N. 2005b. Higher Education and ICT in the Information Society: A Case of UWC, in Erwin, et al, 2005, Community Informatics Research Network (CIRN) 2005 Conference proceedings. Cape Peninsula University of Technology (CPUT), 24 -26 August 2005, Cape Town, South Africa. ISBN 0-620-34769-4

Mlitwa, N. 2006. Information Society Networks, Community Informatics, and Sociotechnical identities: An ANT Perspective. Paper prepared for the CIRN2006 Conference, Monash University, Prato, Italy.

Mlitwa, N. 2007. Technology for teaching and learning in higher education contexts: Activity theory and actor network theory analytical perspectives. Cape Peninsula University of Technology (CPUT): South Africa. IJEDICT, 2007, Volume 3, No. 4, pp. 54-70.

Mlitwa, N. 2010. A Proposed Interpretivist Framework to Research the Adoption of learning Management Systems in Universities. IBIMA Publishing, Volume 1, No. 11, pp. 1-11.

Mlitwa, N. and Birch, D.2008. " Information Security, Access controls and the reliability of Intrusion Detection systems." IST Africa 2008 Conference precedings, 7-9 May 2008, ISBN: 978-1-905824-07-6.

Mlitwa, N., Van Belle, J.P, and Madhusudhan, M. 2009. The use of ICT for Teaching and Learning in South African Higher Education Institutions, 7th Annual Conference on Information Science, Technology & Management Sustaining a Knowledge Economy New Delhi (Gurgaon), India July 13-15.

Mlitwa, N.W.B. 2011. Integration of e-Learning System into Academic Programmes in Modern Universities: A South African Perspective. Cape Town: TVK e-INNOVATIONS.

MSIT **see** Master of Science in Information Technology http://www.floridatechonline.com [accessed on 12 August 2009]

Mugo F. W 2002. Sampling, http://trochim.human.cornell.edu/tutorial/mugo/tutorial.htm (2 of 11) [accessed on 14 June 2012]

Mursu, A., Luukkonen, I., Toivanen, M., and Korpela, M., 2007. Activity Theory in Information Systems Research and Practice: Theoretical Underpinnings for an Information Systems Development Model., Computer Science and IT Centre, Koupio University, Kuopio, Finland, Information Research (IR), Volume 12, No. 3 April 2007, available online at http://informationr.net/ir/123/paper311.html

Nasseh, B 1997. A Brief History of Distance Education; Ball State University, www.seniornet.org/edu/art/history.html [accessed on 11 May 2009].

Neuman, N.L. 2006. Social Research methods: Qualitative and quantitative approaches. Boston, Allyn and Bacon Pearson.

Nichols, M. 2003. A theory for e-Learning Pre-Discussion Paper: eLearning, UCOL Palmerston North, New Zealand, pp. 1-10.

Nonyane, J.N. 2011. ICT Skills Shortages and Capacity Development among Disadvantaged Communities in South Africa: A Case Study of Mpumalanga Municipalities. Unpublished Masters dissertation, Cape Peninsula University of Technology, Cape Town.

Paulins, K. 2010. Information security aspects of e-Learning systems, ICT department, University of Agriculture, Latvia.

Peffers, K. & Ya, T. 2003. "Identifying and Evaluating the Universe of Outlets for Information Systems Research: Ranking the Journals,". Journal of Information Technology Theory and Application (JITTA), 5(1) Article 6. http://aisel.aisnet.org/jitta/vol5/iss1/6 [07 June 2009].

Roos A., 2012 Activity theory as a theoretical framework in the study of information practices in molecular medicine; Hanken School of Economics, Helsinki, Finland and Terkko - Meilahti Campus Library, Helsinki University Library, University of Helsinki; vol. 17 no. 3, September, 2012

Rosswall, T., 1999, The role of ICT in higher education at the beginning of this new millennium. new millennium. Rector of the Swedish University of Agricultural Sciences, in http://online.kennis.org/eva/eva06/ictslu.htm [accessed 15 September 2008]

Savola, R.M. 2009. Identification of basic measurable security components in software intensive systems: Preceding's of *International Social Security Association* (ISSA 2009), Technical Research Centre of Finland.

Scalise S.G.2004. The Future of eLearning in Learning Management Systems, http://www.

Schaefer, T., Barta, M., and Pavone, T. 2009. Student identity verification and the higher education opportunity act: A faculty perspective. *International Journal of Instructional Technology & Distance Education*, *6*(8), Retrieved from http://www.itdl.org/Journal/Aug_09/article05.htm

Schwandt, T.A. 1994. "Constructivist, interpretivist approaches to human inquiry." Pp. 118-137 in N.K. Denzin and Y.S. Lincoln (Editors) Handbook of Qualitative Research. Newbury Park, CA.

Slay, J , and A Koronios 2006. IT Security Risk Management . John Wiley, Brisbane.

Squires, D. 1999. Usability and Educational Software Design: Special Issue of Interacting with Computers, Interacting with Computers Volume 11, No.5, pp. 463-466.

syllabus.com/news_article.asp?id=8901& typeid=155

UCT **see** University of Cape Town https://www.uct.ac.za/ [Viewed on 10 July 2008].

Uden, L., and Kumaresan, 2007.."A usable Collaborative Email Requirements Using Activity Theory," Informatics Volume 31, pp. 71-83.

US **see** University of Stellenbosch http://www.sun.ac.za/ [Viewed on 16 July 2008].

UWC **see** University of Western Cape http://www.uwc.ac.za/ [Viewed on 15 July 2008].

Van Niekerk, J and Von Solms R. 2003 Understanding information security culture: a conceptual framework. Johannesburg, South Africa: *Information Security South Africa* (ISSA), http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/21_Paper.pdf

Vula. **See** University of Cape Town https://vula.uct.ac.za/portal/site/ [18 July 2010]

Vygotsky, L.S. 1978. Mind in society: Development of Higher Psychological Process. Cambridge, MA: Harvard University Press.

Vygotsky, L.S. 1978. Mind in Society: The Development of Higher Psychological Processes; in Cole, M.; John-Steiner, Scribner, S. and Souberman, E. (eds. and trans.), Cambridge, MA, Havard University Press.

Weippl, E., and Ebner, M., 2008. Security and Privacy Challenges in E-Learning 2.0, *Proceedings of earn* 2008, Las Vegas, pp. 4001-4007, 2008, Secure Business Austria / Graz University of Technology, Austria.

Whetten, D.A. 1989. What constitutes theoretical contributions? Academic of Management Review. Vol. 14. 490-495.

William, H., 2003, E-learning tools and technologies: A consumer's guide for trainers, teachers, educators, and instructional designers. Indianapolis, Indiana, Wiley Publishing Inc.

William, R. 2003. Integrating Distributed Learning with just-in-context Knowledge Management. *Electronic Journal of e-Learning*, Volume 1, No. 1, pp. 45–50.

www.ajol.info/index.php/saje/article/viewFile/25046/20717 [29 October 2010].

Yin, R.K.,1994. Case Study Research: Design and Methods; London: Sage.

Abbreviations are used for confidentiality reasons instead of full names of participants.

APPENDICES

Appendix A1: CTS Administrators

Name of participant :..... **Date** :.....

Department :.....

Main Question: How is level of security awareness by administrators?

1. Do you have any workshops or trainings in place for the new network users?(Explain)
2. Do you have any network policies that are guarding misuse by users?
3. If yes, what are those policies? (Email, network, internet, wireless)
4. How do you communicate those polices to departments?
5. How often do you communicate those policies with users?
6. If yes, how often do you conduct training about them?
7. Are you the only department responsible for security of network?
8. What do you do in the case where there are many departments?
9. What security related programs do you have in place?
10. Who facilitate those programs?
11. How do you make sure that those policies are practiced or implemented?
12. Do you have compliance monitoring systems?
13. How do those compliance systems work?
14. How often do network users perform their network compliance?
15. How often do network users complete their computer compliance?
16. Do you block any unnecessary applications?
17. How often do you change your network devices?
18. How do you ensure that the security roles and responsibilities are allocated to officials?
19. What security protection measures do you advise to the network users?
20. Do you encounter network security threats within CPUT network?
21. What kind of threats do you encounter for example (the denial of service, pop up messages, spam, unauthorized access to network, lengthy response time, freezing of computers)?
22. What kind of access hindrances do users mostly report?
23. What problems do those threats cause on the network?
24. If those problems happen, do you communicate them with departments that depend on you?
25. If Yes, How do you communicate those problems to those departments
26. During the maintenance time, do you let your users know in advance?
27. When do you let them know?
28. Have you got the measures in place against those hindrances?

29. How do you make sure that the network is always up to date? (Explain)
30. How do you keep user's computers on a network in good working conditions?
31. What are the criteria for one to get access to network?
32. What do you use to prevent unauthorized access?
33. How are passwords generated?
34. How many characters does a password have?
35. What is the combination of characters?
36. How long do passwords last?
37. How does the unit deal with these breaches?
38. Would you rate the level of performance of network?
39. Are network users satisfied with the performance of the network?
40. If no, what interventions do you have for network cut off during assessment period?
41. Do you receive complaints from lecturers about network performance?
42. What kind of complaints do you get?
43. What do you do with those complaints?
44. If yes, what causes the downtime?
45. Do you communicate the down time causes with the network users in advance?
46. Do you think there is enough bandwidth to accommodate all the users?
47. If No, what causes that?

Appendix A2: Teachers

Name of participant :..... **Date** :.....

Department :.....

E-Learning security measures against unauthorized access

What problems do you usually encounter regarding unauthorized access to course content on WebCT?

1. Lecturers who don't teach the same discipline?
2. Unregistered students?
3. Students who gets assessment tasks before it is given to them?
4. Registered students who have an access to assessment tasks whilst it is still prepared?
5. How are the marks reported to them after an assessment?
6. Are there cases from students about other students who have an access to e-classroom without being registered for the course?
7. **If yes**, how this happens?
8. Does the system always allow you to log in?
9. How long does it take?
10. How many chances are you given to attempt to logging in?
11. As a lecturer, is there a way of ensuring that critical information you have access on is protected from students on WebCT? Eg test, memos (username and password)
12. If yes, what are those ways? (explain)
13. For how long are they used?
14. For username and password, how long must the password be?
15. How is the combination of characters on the password?
16. Do you think it is enough to only have these protection measures?
17. Do you have access rights to download and upload course material?
18. What are these rights for?
19. *If no, who has access rights on your discipline?*
20. Are you always able to upload course material?
21. *If no, what error messages do you get?*
22. Are you always able to download course material?
23. If no, what error messages do you get?
24. How many lecturers are you on your discipline?
25. Who is responsible to post course material? (e.g. coordinator)
26. Do you think it's a right idea to all have posting rights?
27. Do individual lecturers post the course content for all the groups?

28. What happens in the case of the other lecturer having not covered that topic yet?
29. What happens if one of your lecturers has hidden some documents that you have put?
30. What types of data formats do you use on your course material? Explain
31. Can the LMS handle all data types
32. What data format programs have you got in place for your material?
33. Do you have instances with students or lecturers modifying posted course material?
34. If yes, are they supposed to be modifying course material or not (authorized or unauthorized)?
35. What protection measures in place against data modification?
36. What protection measures would you advice in case of data modification? (explain)
37. Are there any protection measures in place against removal of data?
38. What protection measures would you advice in case of removal of data? (explain)
39. Are there any protection measures in place against mis-delivery of information?
40. What protection measures would you advice in case of mis-delivery of information? (explain) different groups
41. What were you trained to use on the LMS?
42. What were you trained on?
43. Who organized the training for you?
44. Rate your level of knowledge about it? (Beginner, mediate ,expect)
45. What do you use the LMS most for? (assessments, notices etc)
46. Are there any challenges you face with its usage? (Explain, what are they)
47. Who do you report those problems to
48. How long do they take to fix those challenges
49. How is LMS operation so far?
50. How are the physical computers protected from theft?
51. Are there any cases where you lost your valuable course information like tests, memos etc stored on your computer before they are given to students?
52. If yes, how? (explain)
53. Is the computer you are using always in good working condition?
54. If yes, how do you ensure that its always in working conditions?
55. *If no, what causes it not to work properly?*
56. Is your antivirus always up to date?
57. Does its performance affect your teaching? (explain)
58. Is there enough bandwidth, and hardware space to accommodate your learning material?
59. Do you experience the cut off during assessment time?
60. If yes, what mechanisms do you have for the assessments when there are cutoffs?
61. Does the responsible department alert you in advance about the cut off?

62. What measures are you referring to?
63. How do you prevent assessment e-Learning system threats?
64. Have you been introduced to blackboard security workshops?
65. What types of security threats are likely happen to your course?
66. What security measures do you normally apply against those threats?
67. What is the difference between your access rights and student access rights?
68. Have students ever tried to write the same online test for more that once?
69. Do you use instant chats with students and peers on WebCT?
70. If yes, how do you communicate with them?
71. If no why?
72. Do you think your students are computer literate?
73. If no, do you think are they aware how assessments are conducted?
74. Have you had any cases where students have failed the test because of not knowing how to use the system?
75. If yes, what interventions have you got for those cases?
76. Do you know of any security policies at CPUT such as (security wireless policy, encryption policy, email usage security policy, internet usage security policy that are guiding you?
77. How are those policies communicated to your departments and students?
78. Are there any security related training workshops about security policies in your department?
79. If yes, how often do you attend those workshops
80. Is the any university security monitoring systems?

Appendix A3: Students

Key Definition

Learning Management System (LMS) – A learning tool that is composed of interrelated components (networked computers, hardware, software, media, procedures of usage and the policies) to ease teaching and learning processes; communicate with others; information sharing (data, images, text, voice and audio); and deliver study material on different data formats at individual's convenience. There are many different LMSs used in Higher Education Institutions in the Western Cape such as (Blackboard, Sakai, Vula etc) but this questionnaire is focusing on Blackboard used at Cape Peninsula University of Technology.

Name of participant :..... **Date** :.....

Department :.....

Section 1:

WebCT Access failure?

1. Does the system always allow you to log in?
2. How long does it take?
3. How many chances are you given for an attempt to logging in?

Passwords as Security measures

4. For how long does your password take to expire?
5. If it's a username and password, how long must the password be?
6. What is the combination of characters on the password?
7. Do you think these security measures are enough as the protection measures?

Upload or download of course material?

8. Are you always able to upload course material?
9. *If no, what error messages do you normally get?*
10. Are you always able to download course material?
11. If no, what error messages do you get?
12. How do you resolve that problem?
13. Do you have instances where students or lecturers modified the posted course material?
14. If yes, are they supposed to be modifying course material or not (authorized or unauthorized)?
15. So on those instances, how do you prevent the modification of data and data format?

Network Security threats

16. What kind of threats do you encounter denial of service, viruses, pop-up messages, spam, and unauthorized access to network?
17. Are there any security measures in place for these threats?
18. How do you communicate them to relevant department?

19. How often do you encounter these threats in a month?
20. How often do you use those measures?

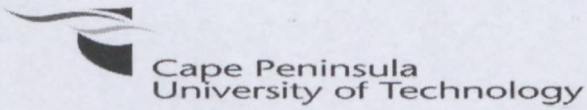
LMS Awareness and its capabilities

21. Training and workshops about the LMS?
22. Have you been trained to use the LMS?
23. What level of training on the LMS do you attend?
24. What are other challenges that you encounter on an LMS in general?
25. Is there enough bandwidth, and hardware space to accommodate your learning material?
26. How often do you encounter hindrances during assessments?
27. How do you prevent assessment e-Learning system threats?
28. Do you do instant chats and online discussion with other students?
29. If yes, how do you communicate with them?
30. If no why?
31. Were you able to use a computer when you started using the LMS?

Section 2: Security Awareness Programmes

32. Do you know of any security policies at CPUT such as (security wireless policy, encryption policy, email usage security policy, internet usage security policy that are guiding you?
33. Have you ever signed any policy document?
34. To what extent are they applied?
35. How were those policies communicated to you?
36. Were there any security related training workshops about security policies in your department?
37. If yes, how often do you attend those workshops
38. Does the university have any security monitoring systems?
39. If yes, how often do you have to comply a year?
40. What are the consequences of not complying?
41. Are those compliance systems improving security in this your department?
42. Are there any policies that guard you against unauthorized modification of course material (Give examples)

Appendix B: Research Consent Letter



No 80 Roeland Street
IT Department Cape Town
Commerce Building Room 1.4

SECURITY CONSIDERATIONS OF E- LEARNING IN HIGHER EDUCATION INSTITUTIONS: A CASE OF CPUT

Dear Student

There is a growing body of knowledge that suggests the significance of e-Learning systems such as Blackboard in supporting teaching and learning processes in modern universities. The benefit of using such systems in teaching (and learning) however, depends largely on whether it is fully accessible, adequately functional and is not subject to undue exposure to computer related security risks and threats.

About the Study

The aim of this research is to understand security issues that affect the day-to-day usage of Blackboard for teaching and learning at CPUT. The idea is to inform improvements at the first instance, and to deliver an academic research output in the form of a master's research thesis, at the second instance.

Request to you

With your considerable experience in the use of Blackboard, we trust that you can share your experiences. **I kindly request your participation in a short research interview (to take place in your office) on security related and practical functionalities of Blackboard**.

About the interview

The interview will take between 20 and 30 minutes. To ensure confidentiality of information, no attempt will be made to identify you with responses you make to the interview. So you free to respond without any fear of victimization. Findings will be used for academic purposes, and recommendations may be used only to inform improvements, with no reference to the identity of the sources. Finally, this research is authorized by, and is in full compliance with the guidelines of the CPUT HDC research ethics committee guidelines.

Thank you for participating

Agreement to participate:

I'm participating in this study out of my free will. I may refuse to participate, or can stop participating at any time, without being penalized for doing so. If I wish, I will be given a copy of this consent.

I,.....hereby accepts the invitation to participate in this research interview as outlined above. Signed at ..... on this _____ day of _____ 2010

Signature_____

Appendix C: Sample of a Transcript

Name of participant : [redacted] **Date : October 2010**

Department : Lecturer Information Technology No of years : 10 Years

What problems do you usually encounter regarding unauthorized access to course content on WebCT?

Lecturers who don't teach the same discipline?

Mak_IT1: No

Unregistered students?

Mak_IT 2: Yes, I have that

I checked my class list and I confronted them. I chased them out of my class and make sure that they do not come back. They had an access to WebCT through their friend's accounts.

How are the marks reported to them after an assessment?

Mak_IT3: Ja sometimes not immediately after the test we give them maybe a day for those maybe who were not there as an opportunity. When we are certain that we are not going to give it again, we show the correct answers and marks. Only when all students are done

WebCT Access failure?

Does the system always allow you to log in?

Mak_IT 5: Well if the system, our system here is not trust worthy cause sometimes is down and we schedule a test and then we have to postpone because of the system that is not or the internet is not working. Sometimes we get email notifications about the systems that will be down.

How long does it take?

Mak_IT 6: Well if the system is up, it takes 1 to 2 minutes, I don't know

How many chances are you given to attempt to logging in?

For me as long as I try, does not limit me I never had situations where it kicked me off because I forgot the password

Do you think it's a right thing to be given those chances? Please elaborate

Mak_IT 7: No its not a good thing because if somebody has an indication of what your password is, he can try many combinations until he gets it right.

What do you think might be causes to take that long?

Mak_IT 8: Ja we encounter a lot of those while the students are attending the test, the pc just freezes and we have to reboot and reset the test for the student to do it again.

How do you think this could be solved?

Mak_IT 9: Well I think ja, its enough, if they can only limit the number of tries

How long must the password be?

Mak_IT10: 8 characters

How is the combination of characters on it?

Mak_IT11: Numbers and characters

Access to subject information? Upload or download of course material?

Do you have access rights to download and upload course material?

Mak_IT11: Yes I do, If I need them I ask, if I need those right I just call her and ask it that please give me those access rights. Then she grants them but she does not take them back after I have used them.

How many lecturers are you on your discipline?

Mak_IT 12: We are 4

Who is responsible to post course material? (e.g. coordinator)

Mak_IT 13: Only the subject head

Do you think it's a right idea to all have posting rights?

Mak_IT 14: Yes, it is right because she will keep track of has been given to the students, the course coordinator will know what, if everyone has a right very soon the course will not be able to control it

Do individual lecturers post the course content for all the groups?

Mak_IT 15: We consult

What happens with the case if the other lecturer has not covered that topic yet?

Mak_IT 16: Well I call her and tell her I need it back

What happens if one of your lecturers has hidden some documents that you have put?

Mak_IT 17: We ask her to put it back

Do you first communicate that with each other before adding stuff on your WebCT?

Mak_IT 18: Not all the time, she puts it and informs us that there is something on WebCT.

What types of data formats do you use on your course material? Explain

Mak_IT 19: Word documents only

Can WebCT handle all data types

Mak_IT 20: Uh, the one I have used, it has handled them

Modification and removal of course material?

Do you have instances with students or lecturers modifying posted course material?

Mak_IT 21: No

If yes, are they supposed to be modifying course material or not (authorized or unauthorized)?

Mak_IT 22: Yes but I have asked for it to be posted back

Are there any protection measures in place against data modification?

Mak_IT 23: Yes with everything by subdividing

Are there any protection measures in place against mis-delivery of information?

Mak_IT 24: There are measures like that by subdividing your class to groups and then allow access rights for the period of time, for that particular group. Only that group will be able to view that information

What protection measures would you advice in case of mis-delivery of information? (explain) different groups

Mak_IT 25: No, Not that I know of

Were you trained to use WebCT?

Mak_IT 26: Yes, I have up to intermediate level

What were you trained on?

Mak_IT 27: On the use of WebCT, putting uploading stuff and all that

Who organized the training for you?

Mak_IT 28: The e-learning center

Rate your level of knowledge about it? (Beginner, mediate ,expect)

Mak_IT 29: Intermediate

What do you use WebCT most for? (assessments, notices etc)

Mak_IT 30: For assignments, notices and sending notices to students, assessments, and also checking material and fun student activities

Are there any challenges you face with its usage? (Explain, what are they)

Mak_IT 30: Well its accessibility, I don't really feel that, the no 1 the labs are not always accessible to students, I think we need a situation where labs are opened 24/7 for students to come at anytime, all the time, am not sure what is happening on their residence as well as the access but I think labs should be available anytime.

What other problems do get then?

Mak_IT 31: Not really I can't think of anything, but freezing of computers

Who do you report those problems to

Mak_IT 32: We report them to the lab technicians and they take a long time to be sorted out and it affects my teaching

How long do they take to fix those challenges

Mak_IT 33: It could be a week, it could be days

When did you start using it?

Mak_IT 34: 6 years ago

How is WebCT operation so far? (poor, good, average, excellent)

Mak_IT 35: Average

How are physical computers protected from theft?

Mak_IT 36: I just save it on my computer and hope that things does not disappear. I only use username and password

Are there any cases where you lost your valuable course information like tests, memos etc stored on your computer before they are given to students? If yes, how? (explain)

Mak_IT 37: Yes we lost practical for students on 1 year that were uploaded on WebCT and we could not retrieve it. I don't know what happened, well lost it and we had to give up and take it as

if it's not been written. Students were supposed to upload their assignment, but students said they did upload, the proof is there that they did upload but the system.

Is the computer you are using always in good working condition?

Mak_IT 38: Not always,

If no, what causes it not to work properly?

Mak_IT 39: I think the internet sometime is the problem, so one will just log on to the workstation might not be able to access the system

How do you keep infected external gadgets (usb etc) away from institution computers? (Explanation, please!)

Mak_IT 40: Well I trust the virus protection programs on my pc that they will be able to scan and remove any viruses.

How do you prevent viruses on your computers?

Mak_IT 41: The programs automatically scan it.

Is your antivirus always up to date?

Mak_IT 42: At some stage it was not up to date, I had to call the technicians to come and fix it

How often to you scan your machine to prevent threats?

Mak_IT 43: I seldom do that

Do you get spam and pop up messages on the computers?

Mak_IT 44: I do,

If Yes, How do you prevent them?

Mak_IT 45: Just delete them as they appear but I never had that case during the assessment time.

How is the network performance in general in CPUT? (poor, good, just fine or average)

Mak_IT 46: Very poor

Does its performance affect your teaching? (explain)

Mak_IT 47: Yes

Is there enough bandwidth, and hardware space to accommodate your learning material?

Mak_IT 48: No

Do you experience the cut off during assessment time?

Mak_IT 49: Yes

If yes, what reservations do you have for the assessments when there are cutoffs?

Mak_IT 50: Well if we can restore the test then we let the student do it again

Does the responsible department alert you in advance about the cut off?

Mak_IT 51: Sometimes not all the time

Do you sometimes encounter denial of service?

Mak_IT 52: No it's only that the service is slow

Have you been introduced to WebCT security workshops?

Mak_IT 53: No

Is security important to WebCT?

Mak_IT 54: Yes

Do you do instant chats with students and peers on WebCT?

Mak_IT55: Yes but not often. But I dint chat with peers

Do you think your students are computer literate?

Mak_IT 56: Not all of them

If no, do you think are they aware how assessments are conducted?

Mak_IT 57: No I don't, if that is considered as training its fine but we tell them what to expect and how to go about it, sometimes we give them a mock test so that they could get a feeling of the system.

Thank you for your cooperation. Be Blessed

Appendix E: Summary of Findings

Table 13: Findings on the Level of LMS Awareness

Theme		Findings (Question = Q; Response = R)	Interpretation
LMS Awareness by users; LMS capabilities and usage: User's knowledge and understanding about the LMS; what they use it for, and application programs used to enhance teaching and learning	Academics	**Q**: Do academics use LMS, what do they use it for? R: "I use it largely in notes, loading and presentation" (PR_TND31) R: "... only notes, announcements and these assignments"(RT_IT56) R: "No, ...but I only using WebCT for announcements, course material" (MB_PR 2) R: "assignments, notices, assessments and fun student activity" (Mak-IT37) R: ..."our system here is not trust worthy..." for example, sometimes "we schedule a test and then we have to postpone because of the system that is not or the internet is not working"(Mak-IT7) R: ..." When it's not up and running, you can't do anything, and even students can't submit assignments" (RT_IT14)... R: "Like I'm not fully reliant on WebCT"(MN_IT21) as a result "I use like handwritten notes" (MN_IT22). **Q**: What LMS access rights do academics have? R: Designer rights (MN_IT46, CST_IT20) R: "Instructor rights" (MM_IT13, PR_TND93) R: is not sure of the access rights (MB_PR8) **Q:** Do you use the LMS for synchronous and asynchronous communication? R: " No, I prefer" using " emails"(CST_IT75, MB_PR46) R: " Yes but not often, but I don't chat with peers" (Mak-IT72) **Q**: Are the students you teach computer literate? R: " Not all of them" are computer literate (Mak-IT73) R: " ... many of them are not computer literate" (CST_IT76) R: " They are literate" (MB_PR48) **Q**: Which academic is responsible for posting course material to the system? R: "Any of the lecturers" (MM_IT14) R: "Only the subject head" (Mak-IT16) R: "...I'm the only one authorized to update and change items on WebCT. (CST_IT 2) **Q**: Can the LMS handle all data types? R: "It should be able to handle (MM_IT22) R: "So I'm not sure if it can handle all the types or what" (MN_IT43) R: " uh the one I have used, it has handled them" (Mak-IT25) **Q**: What application programs do academics mostly use for teaching? R: "On pdf documents" (MB_PR13) R: Powerpoint, any data format depending (MM_IT20, RT_IT30) R: "we give them a spreadsheet" (MN_IT41) R: "Word documents only" (Mak-IT24)	**On LMS awareness by academics, findings suggest that all academics know about the existence of an LMS at CPUT, and they clearly understand its uses and purposes of usage.** On awareness for example, all lecturers were able to make fluent references on what they were using it for, and what they were not able to do with it, which indicates at the very least, knowledge of its existence in the first place. Examples of these statements ranged from claims such as "No ...but I only use WebCT for announcements, course material" (MB_PR 2), to those that say they use it for "assignments, notices, assessments and fun student activity" (Mak-IT37). In addition, functionality complaints that "...system here is not trust worthy..." in that, sometimes "we schedule a test and then we have to postpone because of the system that is not or the internet is not working" (Mak-IT7), suggests awareness. Clearly, one needs to know about the existence of a system and its uses in order to make informed statements such as these. **On the capabilities of the systems, lecturers appeared uncertain about the potential of the current WebCT system to handle forms of data.** Doubts, however, were closely linked to technical failures rather than on the design of the systems. As one lecturer explains for example, "...when it's not up and running, you can't do anything and students can't submit assignments..." (RT_IT14), meaning that when you want to use it at that moment, you are unable to do so. In terms of the features, lecturers believe that an LMS should be able to handle all types of data (MM_IT22; Mak-IT 25), but are unsure of the capabilities of the system at CPUT. Voicing his doubt on this aspect for example, one lecturer said he was "...not sure if it can handle all the types or what" (MN_IT43). Hence, most academics use fewer if not one-application program. Even the communication features were not fully utilized by educators. Whilst an LMS has synchronous communication capabilities, very few educators were fully exploiting these benefits at CPUT. When asked whether they were using the system to communicate synchronously or asynchronously. For example, one lecturer indicated that he uses both formats to only to communicate to students (Mak-IT72). On the other hand, there are who prefer their personal emails instead. Students are also a big part of this LMS usage equation. Whilst students are known to be fluent with the use of new technology including the LMS (MB_PR48), findings for example, suggest that computer literacy for a number of students is also inadequate (Mak-IT73; CST_IT76). This tends to influence the choice of a variety of tools (and depth of their usage) by respective lecturers, lest they risk confusing semi-literate learners of using an LMS to communicate (CST_IT75; MB_PR46). **On whether lecturers were using an LMS for academic purposes at CPUT, findings indicate a very bleak picture.** All lecturers (total n in the sample 8 lecturers) at CPUT were using an LMS for academic purposes. However, the frequency and patterns of usage are limited, incoherent and diverse. In terms of the frequency for example, usage is often inhibited by technical failures as well as inadequacy of features and tool functionality, forcing lecturers to limit their use of an LMS. For example, one lecturer said "...our system here is not trust worthy..."

	Academics *continue…*		sometimes "we schedule a test and then we have to postpone because of the system or the internet that is not working" (Mak-IT7). Uses of tools that are dispersed through an LMS for example, range between "Word documents only" (Mak-IT24), to "pdf documents" (MB_PR13), "spreadsheets" (MN_IT41), as well as power point and any other data format, depending on the type and aim of t he task (MM_IT20, RT_IT30). Even when the system is fully functional however, lecturers only use it for very limited –and hardly similar – purposes. On this aspect for example, one lecturer said, "I use it largely in notes, loading and presentation" (PR_TND31). Another lecturer was only using it for notes, announcements and assignments (RT_IT56). The puzzling aspect of this however, is that limited usage is not a direct consequence of limited rights that educators have in the system. In fact, all educators are granted designer and instructor rights to manipulate all teaching tools in the system, yet they hardly exploit these rights. On this point, one educator stated that educators know and clearly state the rights they have. Academics indicated that they have either designer or instructor rights to the system (MN_IT46, CST_IT20 & MM_IT13). Even with these generous user-rights, there are disciplines where lecturers enjoy full and flexible use of these rights (MM_IT14). There other disciplines too, where only one person (usually the subject head) is allowed to add, remove and edit the course material (Mak-IT16; CST_IT 2).

	Students	**Q**: Do students use LMS on their learning, if yes what do you use it for? R: Check assignments, check the test or sometimes submit assignments (BNJ101; MON34) , R: "Check it for study guides sometimes" (BNJ102) R: "Sometimes we go in and check the marks" (BNJ106) **Q:** Do you do instant chats and online discussions with other students or lecturers? R: 'I don't do that" (BNJ119) R: No, no one uses it (DVD-2n159; BNJ111) R: "I've never use it" (BNJ112) R: "I used it on WebCT" (BNJ 113) **Q**: Have you attended training on how to use the LMS? R: Not really trained as such, not that much (BNJ91; BNJ85) R: "It was just ... " (BNJ 86) R: I was just showed basic stuff like clicking on something and picking subjects there... and was told to find way (MON115) R: "... I had no clue about WebCT... It took me like literally 3 or 4 weeks for each lecture" (MON119) **Q**: Do you find it easy to work on the LMS? R: "It was like blind -pressing for the first time" (ABO17) R: "Struggling, virtually like getting use it" (MON114) R: I knew nothing about the LMS, have attempted and struggled after very long to get to use it (MON116). R: I find it very difficult. It took a time to adjust (MON145). R: We don't know how to use it. We don't have enough information on how to use it (ABO31).	**On LMS awareness by students, findings suggest that they are familiar with the presence of an LMS, and its functions at CPUT.** Indicators of awareness included questions on whether a student was using an LMS, whether the system is easy to use and whether any training have been attended. Whilst these are also indicators of preference and system-literacy, they give a full insight on whether a student is aware of system existence. For example, if one has attended training for the system, know if it is difficult or easy, and be using it, s/he must be aware of its existence. According to the findings, students partially use the LMS for various reasons such as checking learner guides, assignments, tests or their marks (BNJ101; BNJ102; BNJ106). On training, sentiments are that training has been very minimal. One student for example, said "I was just showed basic stuff like clicking on something and picking subjects there... and was told to find my way" (MON115). Even for those who find it difficult, awareness of system presence does emerge strongly. When a student said "...I had no clue about WebCT... It took me like literally 3 or 4 weeks for each lecture" (MON119), and that ""It was like blind -pressing for the first time" (ABO17), reference to the system demonstrate clear awareness of its existence, albeit, with usage master complexities. It is clear therefore, that students are awareness of the learning management system presence on campus. **On LMS communication capabilities, findings indicate that there are LMS features that students do not use at all such as discussion or communication tools.** For example, on their learning, some of the students do not use instant chats or participate in learning discussions with either other students or academics (BNJ119; DVD-2n159; BNJ111; BNJ112). In the same way, some students do explore on the communication features (BNJ 113). **In terms of computer skills, training, and easy usage of the LMS, findings reveal that d**espite the fact that students use WebCT, it is clear that most students never had an opportunity to attend training for beginners on how to use or interact with the system (BNJ91; BNJ85). However, that has hindered the overwhelming functionality and usefulness of the LMS for learning purposes. For example, some of the student had never touched or worked on a computer system before (ABO17). On that note, it made it difficult for students to interact with the computer system, let alone doing LMS activities (ABO31). However, for those students who were fortunate enough to attend LMS beginner's workshop, were just introduced to the very basic usage of the system (BNJ 86; MON115). In fact, most of these students indicated that they never really attended concrete foundation on training about the usage of the system. For instance, "Struggling, virtually like getting use it" (MON114) and I knew nothing about the LMS, have attempted and struggled after very long to get to use it (MON116). However, some students had no idea about the system, let alone interacting to achieve learning. For example, it literally took 3 to 4 weeks for each lecturer (MON119). For other students, it was their first time to touch the computer. One student explained that it took him time to adjust (MON145) and another student contends, "We don't know how to use it. We don't have enough information on how to use it" (ABO31).

Table 14: Findings on current LMS security programs, rules, and procedures

Theme		Findings (Question = Q; Response = R)	Interpretation
LMS awareness programs in place : Introductory workshops, policies, guiding rules, procedures and compliance system	Academics	**Q**: Have you attended any LMS training? If Yes, rate your level of understanding. R: "No" (MM_IT10) R: "Yes, I'm a Beginner" (PR_TND30) R: Yes, have up to intermediate level (Mak-IT33, CST_IT47) **Q**: Have you been introduced to any LMS security usage rules, policies and procedures? R: don't know of any polices (PR_TND40; MB_PR49; RT_IT 119) R: "There should be, but I'm not as updated as I should be about policies. So, not that I know of, but I'm sure there should be (CST_IT81) **Q**: If Yes, which CPUT security policies were you introduced to? R: "...there is definitely a policy posted on the website against email usage definitely" (CST_IT39)	**On literacy, introductory workshops and training by academics, findings suggest different levels of competency that affect LMS usage.** Whilst CPUT lecturers have access to the LMS, it is clear from contrasting responses that some of the academics never attended an introductory training or workshop about the use of the system (MM_IT10). However, some of the academics who attended the LMS induction workshop do not have confidence in adopting and using the LMS. The cause of the minimal adoption and usage of the system could be caused by the academic competency as some have either gained elementary skills (PR_TND30) and intermediate skills (Mak-IT33, CST_IT47) to use the e-Learning system. **On whether supporting security policies, rules and procedures exist, judgments reveal that academics are not fully aware of the guiding rules, procedures and compliance system.** For instance, even when some of the lecturers have attended the LMS orientation training, some of them are not familiar with any guiding network security policies, procedures and rules (PR_TND40; MB_PR49; RT_IT 119). In contrast, some other lecturers assume that "there should be, but I'm not as updated as I should be about policies. So, not that I know of, but I'm sure there should be" (CST_IT81). Findings clearly show that most if not all academics have not responded to the follow up questions on policy usage and other factors because of the lack of awareness about the policies.

	Students	**Q**: Have you been introduced to any LMS security usage rules, policies and procedures? R: We never had orientation about WebCT(DVD-2n108; BNJ125; MON154; MON155; MON156 MON157; MON158) R: There was something at the beginning of the year (BNJ126; DVD-2n107) R: "I think it was about WebCT I'm not sure" (BNJ127) R: I don't know of any policy. I don't know if they exist (MON150). **Q**: If Yes, which CPUT security policies were you introduced to? R:?? (no response) R:?? (no response) **Q**: Have you ever signed LMS security compliance forms, and how often a year? R: "No, we signed compliance forms in our first year saying that we will not to destroy property of CPUT" (DVD-2n181) R: I don't even think they ever had (DVD-2n 184) **Q**: Are these policies improving LMS and network security within the campus? R: We know nothing of the compliance of it. (DVD-2n183; ABO 35)	**Findings indicate indistinctive results about LMS Introductory workshops for students.** For example, despise an overwhelming usage of the LMS by students; awareness about network security policies, rules and procedures ranges from non-existent to minimal. However, some students cited that they did not have the orientation time (DVD-2n108; BNJ125; MON154; MON155; MON156 MON157; MON158). Some of those who attended a training at the beginning of the year are not even aware of what they have attended (BNJ126; DVD-2n107). For example, when asked to describe the training on LMS usage and security compliance they received, the most that the two students could say was there was something at the beginning of the year (BNJ126; DVD-2n107), but could not even remember its name or description. Parallel with this concern is that another student who claims that he does not know of any policy (MON150). **On existence of supporting security policies, rules, procedures and security compliance forms, judgments indicate student's unclear understanding about security measures.** Whilst every registered student has an access to the physical resources (computer, network and LMS among others), students were asked if they have ever complied with the resource usage (network and LMS policies). One student responded that he signed a form on the first year level for protection of the property. Another student contends and assumes that the university has never had compliance system (DVD-2n 184), as they claim that they know nothing about LMS and network security. In their understanding, they do not believe that policies exist in any case (MON150). However, its only one student who recalls if they signed forms from the beginning of the year, though he is not sure if they were security compliance related. For example, "No, we signed compliance forms in our first year saying that we will not to destroy property of CPUT" (DVD-2n181). Another student does not even think that the university ever had that (DVD-2n 184). This has however made it difficult to judge its impact and importance on the LMS usage(DVD-2n183; ABO 35).

	Network administrators	**Q**: Do you have any policies in place that are guarding the use of the network? R: "Ja,ja,we've got policies,ja" (OF_NET64) **Q**: How do you communicate security measures, policies, rules and procedures to network users? R: "they are normally communicated. Some of them are on the webpage" (OF_NET65) R: " ... or its published on the web, if emails are sent out or on staff notices (OF_NET67) **Q**: Are there any workshops conducted for new network users? R: Students get through their induction (OF_NET66). **Q**: Who facilitate those workshops? R: "We try to educate the users"(OF_NET48) **Q**: Do you sometimes experience people who breach security policies? R: " ... there's always people working at breaching security" (OF_NET63)	**In terms of current supporting security policies, rules and procedures by network administrators, findings reveal that** e-Learning system comprises on many aspects, where network forms an integral part of the system (OF_NET59). When asked if there are any policies in place that are guarding the usage of the network, an administrator said, "... we've got policies, ja" (OF_NET64). **In terms of communicating the current security measures to users by network administrators, h**owever, findings show that the network department is responsible for communicating security policies, rules, procedures to network users. This department is striving to send security information through posting on webpages, email as well as staff notices (OF_NET65; OF_NET67). **On whether introductory workshops, induction exists and monitoring of policies by network administrators, findings reveal that w**ith students, these guarding security policies communicated through workshops after their registration, and during the induction process (OF_NET66). Even though security network administration team is making efforts to make network users aware of the security guarding policies, and other protection measures, there are always people working at breaching security" (OF_NET63). For example, the network administrator clearly declared they "try to educate the users" (OF_NET48).

Table 15: Findings on LMS Security Threats

Theme	**Findings** (Question = Q; Response = R)	Interpretation

Existing LMS Security Threats and user challenges: Hindrances such as viruses pop up messages, denial of services, lengthy response time, and user challenges about online tests.	Academics	**Q**: Do academics encounter any problems relating the LMS usage? R: "... takes long to actually attach a file, but sometimes it won't attach it at all. It just get stuck and then eventually it bombs out" (CST_IT21), "...it was slow and its unstable and we don't trust it with tests"(CST_IT73) R: " Well its accessibility, ... we need a situation where labs are opened 24/7 for students to come at any time ..." (Mak-IT44) **Q:** What types of computer and network problems do you get? Please explain R: ": It's just those messages" that are "destructive very much" (MB_PR30) that say the computer will restart your computer" (MB_PR29). He uses "a very old computer that is slow and makes noise, its sticks like most of the time" (MB_PR25) R: "... freezing of computers" (Mak-IT39) and network is Very poor (Mak-IT54) **Q:** Do you encounter hindrances such as viruses, pop up messages, etc? R: "Just delete them as they appear" (Mak-IT53) R: "At times I've noticed that when that pop-up block come up and they say they are not registered or they can't access their email" (PR_TND99) R: "...since there are multiple viruses on the network. Our pc's are never safe, anything from students. The chances of you getting a virus are very high. Not even receiving items from students, but logging into the network and on its own is a risk" (CST-52). **Q**: To whom do you report challenges to? R: "I used to report it to the WebCT department... but I don't do that anymore" (CST_IT22) R: "I reported the issue, there was a lecturer who was given a task to orient me" (MB_PR10) R: "We report them to the lab technicians" (Mak-IT40) R: "Nah, I don't" (PR_TND33) **Q**: And how long do those challenges take to be fixed? R: "They take a few hours" (RTR_IT61) R: "It could be a week, it could be days" (Mak-IT41) **Q**: What experiences do academics have relating to LMS online assessments? R: "No, ...I don't use online assignment. I hardly make use of WebCT"(PR_TND65) R: "Yes, Well if we can restore the test then we let student do it again"(Mak-IT58, Mak-IT59). **Q**: Do academics encounter students with unauthorized access and are registered but have no access to the LMS? If Yes how? R: "Yes, I have that", "I checked my class list and I confronted them. I chased them out of my class and make sure that they do not come back. They had an access to WebCT through their friend's accounts" (Mak-IT2) R: "There are students who, in class who failed to access WebCT, I don't know the reason why, because some of them you try to upload them but the system does not pick them up. so I had a couple of them" (MB_PR1) R: "……so at some stage, I had to give him my password, so he could have the password to access WebCT" (RT_IT2) R: "……I haven't come across" (MN_IT2) R: "Not that I remember" (MN_IT10)	**In terms of security threats and hindrances on LMS usage by academics, f**indings clearly indicate that LMS adopted in CPUT sometimes does not operate as expected by users due to existing security threats and disturbing hindrances. However, these challenges vary from LMS functionality and usability, resource or network problems and destructive pop up messages among others. As a result these challenges are discouraging LMS users by obstructing the services. For example, one of the lecturers commented that, the LMS is hopelessly slow and unstable as a result, she does not trust it for assessments (CST_IT73). This lecturer further explained that when working on the LMS, it"... takes long to actually attach a file, but sometimes it won't attach it at all, it just get stuck and then eventually it bombs out" (CST_IT21). **For computer and network security related threats and hindrances, judgments reveal that o**ther lecturers are using noisy and "old and computers" that often freezes on a slow network (Mak-IT54; MB_PR25). Likewise, some of academics suspected that the slow level of LMS operation emerges from multiple viruses that congest the network as well as interrupting pop up messages that directly affects the usage of the system (MB_PR29; Mak-IT53; PR_TND99; CST-52). However, sometimes students do not get enough time to access the LMS due to unavailability and locking of the labs after classes (Mak-IT44). **On whether academics report these LMS security challenges, findings revealed that w**hen these disturbing threats and hindrances constantly happen, they discourage LMS users to an extent that one lecturer does not bother to report the problems anymore (CST_IT22). Whilst one other lecturer still hopes that the situation will change by reporting them to lab technicians (Mak-IT40). Some of the lecturers are not even sure of the duration for the problem to be solved (Mak-IT41). **In terms of challenges based on online assessments and unauthorized LMS access, academics report that, a**s much as the LMS provides unstable environment, some of the academics indicated that they do not use the LMS for assessments because it is not trusted. As a results one lecturer uses it for assessment purposes, but he always have alternate ways to cover in the case of cut offs (Mak-IT59, PR_TND65). These challenges that academics encounter are not only limited to the use of the system but rather expand to access of eligible students to the system to access learning material through the peer assistances (Mak-IT2) and registered students submitting their own work on another peoples name (RT_IT4). However, the system sometimes would not allow some academics to enroll students who are registered (MB_PR1), whereas other

	Students	R: ".....I had students who could submit in another person's name, and write even a letter, to explain that I have submitted in this name because I am not yet registered" (RT_IT4) **Q**: What comments have you got relating to LMS usage experiences? R: "I can't log in for the past couple of weeks" (MON75) R: I did not have any subjects on my LMS page (MON120). R: We assume that many of our Lecturers do not use the LMS and most of its features (MON123; MON131). R: Difficulty with uploading stuff on WebCT and sometimes links get missing (MON127) R: We just expected the interface to be more efficient, to be more attractive, we only go online when we need to download stuff (MON109). R: LMS is just so basic; we expect something much more than what things are now (MON110) R: Difficulty with login on WebCT (MON49) **Q**: Are you always able to download and upload material on the LMS? R: "Sometimes you can upload" (ABO1) R: "No, I never uploaded, but downloaded" (MON83) **Q**: If No, what kind of problems or errors do they encounter. R: You cannot submit and you get 5 to 30 marks deducted because of that (BNJ4; DVD-2n27; DVD-2n26; DVD-2n26). R: "Submit a file and the receiver will get it corrupt, until I ended up using my friends account" (DVD-2n 39) R: Sometimes you get a problem of downloading document on 2010 with 2003 and it takes a lot of time that you don't want to waste and that's a format error and its annoying (BNJ43; DVD-2n37; DVD-2n 45) **Q:** What types of computer and network problems do you get? Please explain R: The network is always infected with viruses, even when you still login on the computer (DVD-2n 72) R: "Which is time consuming" (DVD-2n 90) R: "Slow and annoying sometimes" (DVD-2n 205) R: many different passwords used to access the system (MON146) **Q:** Do you encounter hindrances such as viruses, pop up messages, etc? R: "... that java thing, when you open WebCT. Then you get You- that come up. You can run java or cancel it" (BNJ76) R: "It's just annoying every time you have to go click, click, click. It's now become second nature that we just do it" (DVD-2n 87) R: "Ja, but the big issue is whenever you want to download it takes you right back and you have to go all the way" (DVD-2n 32; DVD-2n29). R: "WebCT and the pc's at this university are virus infected" (DVD-2n60). **Q**: And how long do those challenges take to be fixed? R: "they change your password" (MON17) R: "Immediately" (MON20)	academics on the same discipline would share the access details with each other (RT_IT2). **For LMS security user challenges and experiences, findings by students report that w**hilst CPUT has adopted WebCT LMS for teaching and learning purposes, security threats are the most cited inhibitors on the LMS usage by students. Security related experiences that students encounter vary from one student to another. For example, a complaint is that the LMS access denied to some students or number of weeks (MON75, MON49). However, when they have an access to the LMS, students encounter difficulty in uploading documents or locating to necessary links that are sometimes get missing (MON127). In fact, to some registered students LMS homepages do not show currently registered subjects (MON120). Judging from a number of negative experiences reported by students, an unclear LMS interface and academic flexibility and interaction to the system is evident. LMS interface seems not to be as a clear, attracting and guiding tool. To students, it seems as a very basic tool as they expect something more interesting and attracting especial on their IT field of study (MON110). Assumptions are academics do not fully use the LMS features to enhance their teaching (MON123; MON131). It is evident that some of the students "never uploaded" (MON83) documents but have made use of the download feature (MON83; ABO1). Findings are clear that students are hindered in many ways from when using a submit task feature. For example, many students complain that when submitting a task, the system blocks students and they are penalized about that by losing many marks (BNJ4; DVD-2n27; DVD-2n26; DVD-2n26). Sometimes the system allows them to submit a file but the receiver will get it corrupted until students use other peoples account to submit the file. In addition, incompatibility of the applications used also one of the major concerns (BNJ43; DVD-2n37; DVD-2n 45). **Findings about computer and network security inhibiting factors clearly show that** security threats are not limited to the LMS usage but include computer and network challenges as well as inhibiting factors such as viruses, denial of service and destructive pop up messages. For example, one students claims that "The network is always infected with viruses, even when you still login on the computer" (DVD-2n 72). It is evident that presence of these viruses on the network is "time consuming" (DVD-2n 90); which causes the network to be "Slow and annoying sometimes" (DVD-2n 205). In addition, students use many different passwords to access just the computer (MON146). However, pop up messages are confusing and disturbing to many students,

	Students continue...	**Q**: What experiences do students have relating to LMS online assessments? R: "You just read the instructions and you go off" (DVD-2n 112) R: "It will crash, then it doesn't send it straight through your page doesn't refresh" (DVD-2n 118) R: "The session is being ended" (DVD-2n 222). R: "Yeah, and then you have to start almost from the beginning" (DVD-2n 223)	**Findings by students about help desk response time show that** student's problems are mostly password related. However the responsible department sometimes fixes the problem immediately (MON20) or "they change your password" (MON17) **In terms of students experience about online assessments, findings clearly indicate t**hat the LMS sometimes constantly crashes whilst students are busy with the assessments (DVD-2n 118). As a result, students are forced to start the assessment over, from the beginning (DVD-2n 223). However students would be cut off by the LMS in the beginning or middle of the assessment, for example, one student would just read the instructions and page would go off (DVD-2n 112) or would receive a message indicating that the session is ending (DVD-2n 222) . As a result, when the assessment page would just freeze, does not refresh(DVD-2n 118)
	Network Administrator	**Q**: Do you recall any instance where network users encountered any challenges in using the system? R: " I think the network is a very crucial element in this, specifically with e-learning and stuff like that, so the network is crucial (OF_NET59). R: "... the network is slow" (OF_NET56)R: "it slowed down the mail, server (OF_NET14) R: "They have been complaining that their network is slow" (OF_NET18) **Q**: What kind of network security threats do you encounter on CPUT network? R: " That's mostly viruses, worms and stuff like that" (OF_NET4) R: " ... the email server was a denial of service" (OF_NET13) **Q**: What problems do those threats cause on the network? R: ... the CPU went up to 99% so we could not do stuff, it slowed down the mail, server (OF_NET14) **Q**: Have you encountered a case where unauthorized people intruded on the system? R: "... there was some users downloading stuff from somewhere..." (OF_NET18)	**In terms of user's challenges on the system, findings report that C**PUT network administrator commented, "... the network is a very crucial element in this, specifically with e-learning and stuff like that, so the network is crucial (OF_NET59). However, the network functionality, response is hindering, restricting and controlling the service to users. Findings show that LMS users often complain about the functionality of the network. For example, the network administrator said, "They have been complaining that their network is slow" (OF_NET18). In fact, the network does not only affect e-Learning systems but directly affects other network services, such as mail server that is slow or not accessible at all (OF_NET14). **For network security threats by network administrators, f**indings reveal viruses, worms and denial of service as the common threats that cause the instability of the network (OF_NET4; OF_NET13). When these challenges arise on the system, they obstruct, adjust and directly affect system settings block the service to an extent that users and network administrators could not do anything (OF_NET14). **In terms of unauthorized access to the system, findings by the network administrator indicate that t**here are unauthorized people who contribute to the poor level of network services by accessing, misusing, exhausting the network bandwidth (OF_NET18).

	CTS technician	**Q**: How many employees are within your department? R: Business administration has 4, networking and service desk has 8 and end user computing has 16 (ZN_5) **Q**: Do you think you are enough for the work load the department has? R: "No, because we are rendering a service to 34000 students, 5000 contract and permanent staff in 11 campuses and +- 30 residences" (ZN_6) and "It's difficult to provide a service quick to clients due to the number of network users we have" (ZN_7) **Q**: What challenges did you encounter after the merger? R: "Centralized services example is ITS system is managed in Bellville campus only; staffing shortages" (ZN_14) R: "... relocating staff between campuses to help ease the workload . **Q**: Has your workload changed after the merger? R: "Yes, due to bigger systems & bigger user base" (ZN_17)	**In terms of network access and usage experiences by CTS technicians,** findings show that there are only 28 employees within the CTS department (ZN_5). All these personnel's are divided among 11 CPUT campuses (ZN_9). However, the limited number of these employees makes it difficult to service 39000 staff in all the campuses including +- 30 student residence. On this account, the technicians feel that there is a huge shortage of staff within the department. For example, each campus has only 2 end user technicians allocated to it.

Table 16: Findings on LMS Security Measures and their implementation

Theme	**Findings** (Question = Q; Response = R)	Interpretation

Security Measures used and the extent of their implementation: Practical precautions to avert www network related risks to information over an LMS.	Academics	**Q**: How do academics protect critical information on the system such as tests, memos etc.? R: " I just save it on my computer and hope that things does not disappear" (Mak-IT44) **Q**: How long are the LMS passwords and their combinations? R: "8 characters" (MM_IT10) R: "6 letters, No numbers" (RT_IT45) R: "10 letters" (MB_PR6), Its only letters (MB_PR5) **Q**: How long does it take the login details to expire? R: "Mine lasts forever … I've had the same since last year" (CST_IT17) R: "I never changed it the whole year" (MB_PR4) R: "I just change it always to maintain my password" (MM_IT10) **Q**: What measures do you think should be implemented to protect critical information? R: "…there should be a way to use to secure your files as well to put a password specifically on an assignment... With assessments for every assessment you do you can save it with a separate password" (CST_IT19). R: "I would prefer to have 3 chances to use the protection measures" (MB_PR4). R: " Change password monthly" (MM_IT11) R: " If they could reduce the number of tries" (Mak-IT12) **Q**: What are the measures used against access hindrances (spamming, viruses and denial of service etc.) R: "Well I trust the virus protection programs on my pc that they will be able to scan and remove any viruses" (Mak-IT48) R: "… you can scan for them and have them quarantined or remove possible" (CST_IT54) , "I block the spam as far as possible" (CST_IT57) **Q**: Are they always up to date? How often do they update them? R:: "I update my antivirus once maybe in 6 months" (MB_PR28) R: "I usually update it myself if it's not updated" (RT_IT 70) R: "At some stage it was not up to date, I had to call the technicians to come and fix it and I seldom update" (Mak-IT50, mak-IT51) R: " It used to be, but lately it doesn't seem as if my antivirus is updating" (CST_IT55) R: "I don't even have an antivirus" (PR_TND40) **Q**: Who is responsible to update the system? R: "I usually update it" (RT_IT 69)	**Whether there are any current measures to protect critical information on the system by academics, findings show that there are m**any factors cause an ideal LMS to offer effective benefits to its users. Safety precautions are one of major security issues that should be highly considered on an e-Learning system. Protected and secured platform enables users to perform their activities that will achieve a highly desired outcome. In addition, it makes users to rely on that kind of environment. For example, one of the lecturers trusts that information stored on a computer is safe and hope that it can never disappear (Mak-IT44). **In terms of current login security measures, judgments reveal that p**assword considered as one of the measures used to secure a learning platform. When academics asked how their password combinations are, some reported that they mostly use the alphabet only. For example, one lecturer indicated that his password 8 characters long (MM_IT10). It is clear that lecturers generally use passwords varying from 6 letters to 10 letters only. **In reference to extent of implementation of the current security measures, findings revealed that s**ecurity measures implemented works effectively when they are revised constantly as to reduce chances of intrusion and easy password guessing. However, some of the lecturers never changed their passwords. There is one-lecturer that has never changed her password "Mine last forever" (CST_IT17) whereas others constantly change it to maintain security issues (MM_IT10). As much as there are safety measures in place, it is ignored that they need to be maintained. As a result some lecturers mentioned that these measures are not always not always up to date (Mak-IT50 ; Mak-IT51) and one other lecturer normally update it the system herself (RT_IT 70). However, other lecturers do not even have the antivirus installed on their computers (PR_TND40) and another lecturer updates it "maybe in 6 months" (MB_PR28). Interconnected computers are supposed to be preloaded with security measures that secure and protect the usage and functionality of the network. Some of the academics rely fully on the current security measures, for example, one lecturer using LMS for his teaching commented, "Well I trust the virus protection programs on my pc that they will be able to scan and remove any viruses" (Mak-IT48). Another lecturer believes and trusts that viruses can be "quarantined and removed" (CST_IT54). However, some of the lecturers take extra precautions by blocking and avoiding interruptive spam messages (CST_IT57). **Findings show that academics have recommended some security measures that they would prefer.** When asked to recommend precaution measures to protect critical information on the LMS, one academic suggested the use of separate passwords when storing files and documents and a common password that will be shared among user of that specific file (CST_IT19). However, other lecturers felt that changing of passwords regularly and a limited number of log in times would help on this matter. (MM_IT11; Mak-IT12; MB_PR4).

	Students	**Q**: How long are the LMS passwords and their combinations? R: 6 or 7 numbers (BNJ19; BNJ20;BNJ22; DVD-2n21; DVD-2n24; MON23; BNJ21) R: 10 to 14 characters (DVD-2n18, DVD-2n19; DVD-2n20; MON21) R: combination of alphabets, numbers and symbols (DVD-2n23) **Q**: How long do login details last? R: On WebCT you don't change your password (BNJ 25; MON30) R: " I don't use that option to change password" (BNJ26) R: No, they don't ask you, you can keep it for a whole year (MON29; MON28; MON32) **Q**: Do you think it's a good idea, and why? R: No it's not too good, because then everyone can see your password and then try to use it (BNJ 28; BNJ29) R: "Carried over from last year" (DVD-2n203). R: I've changed mine the beginning of this year (DVD-2n 204)R: There is a change password option but it doesn't work (BNJ30, BNJ31) **Q**: What are the measures used against access hindrances (spamming, viruses and denial of service etc.) R: You just clean up the pop up message… (MON98) R: "They're always there" (MON99) **Q**: What would you suggest, as a way of improving LMS usage, network and security? R: It should be more user-friendly (BNJ 93; BNJ 128) R: Updating of the grade book and interface (BNJ130; BNJ98) R: LMS password should be changed at least once a month or once a quarter (DVD-2n 188; MON36; DVD-2n 189) and synchronize the network password with the LMS password (MON160). R: … that student must be trained on how to use the LMS (MON118) and I think more training for both students and Lecturers (MON160). R: It is the functionality (MON164).	**Findings in terms of login security measures** show that students take precautions to protect their information on the system. However, responses on the LMS password combination and length vary from a plane numbers, alphabet and symbols to a combination of them all (DVD-2n23). As a results, many students claims that they use a range from 6 to 7 plane numbers (BNJ19; BNJ20;BNJ22; DVD-2n21; DVD-2n24; MON23; BNJ21) to 10 to 14 characters (DVD-2n18, DVD-2n19; DVD-2n20; MON21). **However, in terms of the extent of implementation of those measures, findings reveal that** it is clear that all students are actively using protective measures such passwords when accessing the LMS. However, it is surprising that the usage of the security measure is not maintained. From the number of responses, it is evident that students do not change the password on WebCT (BNJ 25; MON30). Other students do not use the change password option on the LMS (BNJ26). In fact, the system does not send a notification reminder that the password has expired. As a result, students use the password for the completely academic year (MON29; MON28; MON32). When asked their opinion about using the same password for a very long time, they responded that it is not a good thing to do as it increases chances password hacking (BNJ 28; BNJ29). In contrast, other students believe that there is an option on the system but it is inactive (BNJ30, BNJ31). However, some students claim that their passwords are "carried over from last year" (DVD-2n203). **In reference to current security measures against access hindrances, findings show that** even though students strive to protect their information when they login on the system, there are still hindrances that inhibit they on using the LMS such as viruses, spam mails and denial of service. As a result, students turn to make peace with those distracting pop up messages. For example, some students commented that those messages are always there (MON99) so they just clean them up (MON98). **Results show that students shared their suggestions on how they would want the current LMS functionality**, usage, network and security to be improved. An attention stood out on the LMS interface to be more user friendly(BNJ 93; BNJ 128); that there should be a clear LMS functionality and features such as grade book should always be up to date(MON164;BNJ130; BNJ98). Despise the interface of the LMS, students pointed literacy for both students and lecturers (MON118); and user access with synchronized network and LMS passwords (DVD-2n 188; MON36; DVD-2n 189) that should be changed at least once a month (MON160).

	Network Administrator	**Q**: What security measures do you have in places for the current threats? R: " We are using McAfee… try another like AVG" (OF_NET9) R: " … we've got some tools that we 're using now, ja sniffing tools" (OF_NET18) R: " We've got 2 firewalls" (OF_NET26) **Q**: How often are the measures updated? R: " … you have to update almost every day" (OF_NET12) R: " Well, the way that thing is set up, its setup correctly, to automatic scan" (OF_NET8) **Q**: Who is eligible to use the network? R: " You need to be a registered student" (OF_NET23) **Q**: How long are they and their combination? R: "The password should be 8 characters or longer…" (OF_NET38) **Q**: How long do those password measures last? R: "I think it is 4 weeks or 6 weeks…" (OF_NET39) **Q**: Is there current system to monitor the network usage and compliance system? R: 'We can see on OPA where it's been used" (OF_NET41) **Q**: What do you do to improve security of the network? R: "…It's something we always look at, updating stuff, doing new things" (OF_NET63) **Q**: What do you do in the case of network policy breaches? R: " … we disable their accounts or stuff like that" (OF_NET71) **Q**: How do you ensure that computers are always in good working order? R:" … I think we've got a 4 year" if it's not 5 year renewal plan for computers (OF_NET28) **Q**: How do you ensure that the network is always up and running? R: … we continually improve bandwidth and do things to limit people from abusing it (OF_NET30)	**In terms of current security measures, n**etwork administrator claims that the university has security measures in place for the current threats that both academics and students are experiencing. However they use McAfee, in the case of failure they use and another measure e.g. AVG (OF_NET9). The network is further protected using sniffing tools (OF_NET18) and (two) 2 firewalls (OF_NET26). **However on extent of implementation of the current security measures, network administrator explained that** "… you have to update almost every day" (OF_NET12). In addition, some of these measures are set to scan automatically for any disturbing and hindering factor on the network (OF_NET8). The network administrator declares that only registered CPUT students who are eligible to have an access to the network. Once students are registered, the get the password and the username to use when accessing the network. However, the network password is designed to be at least 8 characters or long (OF_NET23; OF_NET38). When accurately used, the login details should last for at least four (4) or six (6) weeks (OF_NET39). In the case of network misuse, the technical department does not have a security compliance system but has monitoring software that is incorporated on (Online Personal Access) OPA system to trace the event. For example, "We can see on OPA where it's been used" (OF_NET41). In the climate of various affecting factors such as (slow, unstable networks), the networking department claims to be in a lookout, updating and doing new things to improve the level of the security network (OF_NET63). In the case of network policy and security breach, the department takes protective measures by disabling the intruder's account (OF_NET71). The network security administrative team service and maintain both university computers and the network. However, with computers, CPUT has a four (4) or five (5) year renewal plan of computers (OF_NET28). Likewise, with the network, the department strives to "continually improve bandwidth and do things to limit people from abusing it (OF_NET30).

Table 17: Findings on LMS User Access

Theme		Findings (Question = Q; Response = R)	Interpretation
LMS user access: Security related issues of access & use	Academics	**Q**: Does the LMS always allow academics to easily login, If NO, what challenges do you encounter? R: "It depends. Sometimes WebCT is very slow and takes forever to log in. Other days it's fast. I think it depends on the network. Last year we had quite a bit of problems with it being very slow (CST_IT7). R: "Some days when Webct's down, you can't log into it"(RT_IT10) R: I don't remember a case where I log in and it doesn't allow me in, except if I type the wrong passwords (MN_IT13) **Q**: How long does the LMS take to grant academic an access to the system? R:" ... in the labs it takes more than 2 minutes wait to log in. Even up to this day it still takes too long" (RT_IT11) R: "if the system is up, it takes 1 to 2 minutes, I don't know" (Mak-IT8); R: "Currently 5 minutes,...I don't have to wait more than 5 minutes" (PR_TND6) **Q**: How many times can an academic attempt to login on the system? R: "For me as long as I try, does not limit me I never had situations where it kicked me off because I forgot the password" (Mak-IT9) R: "3 times, about 3 times... then it goes off" (MN_IT15), If I go 2 times, then I just go straight to forget your password. I'm not sure how many times does it allow you. I'm not sure how many attempts does it give you (MN_IT19). **Q**: What are the causes of these access errors & problems? R: "I'm not sure. It doesn't give a password error. It doesn't give an error with my user name. So it's just give that screen again where you log in. It just looping to that screen it doesn't really display anything"(CST_IT12)". . I think it depends on the network or what (CST_IT7)... "Their Java interface that we had only for WebCT is the old one" (CST_IT12). R: ..."Sometimes it's slow, that could be a technical problem" (MN_IT21) R: "I don't know what affects that"(RT_IT14) **Q**: What is the impact of this on teaching & learning? R: ..."our system here is not trust worthy..." for example, sometimes "we schedule a test and then we have to postpone because of the system that is not or the internet is not working"(Mak-IT7) R: ..." When it's not up and running, you can't do anything, and even students can't submit assignments" (RT_IT14)... "Then you cancel that lecture and say this is the reason to that group (RT_IT15). R: ..."While students are attending the test, the pc just freezes and we have to reboot and reset the test"(Mak-IT11) R: "Like I'm not fully reliant on WebCT"(MN_IT21) as a result " I use like handwritten notes" (MN_IT22)	**Findings about LMS user LMS access and usage by academics reveal that s**ecurity limitations are a major impediment rather than an enabler of LMS access and usage by academics at CPUT. When asked whether academics are able to login without hindrances, one academic complained that "sometimes WebCT is very slow and takes forever to log in..." and in the previous year there were "quite a bit of problems with it being very slow" (CST_IT7). Another lecturer adds that in "some days when WebCT's down, you can't log into it" (RT_IT10), which means a complete lack of access. Under normal circumstances, it takes over 2 minutes (RT_IT11; Mak-IT8), and sometimes 5 minutes (PR_TND6) to complete a login in computer labs. Of major concern is that often lecturers do not know the causes of these problems (RT_IT14; CST_IT12). In the words of another lecturer for example, "it doesn't give a password error. It doesn't give an error with my user name. So it just give that screen again where you log in. It just looping to that screen it doesn't really display anything"(CST_IT12)". Close guesses are that "it depends on the network or what (CST_IT7)..." and that existing software may be outdated (CST_IT12). When security problems hinder access to, and performance of an LMS, this has a negative impact on system usage for teaching and learning. On this point, one lecturer said "...our system here is not trust worthy..." for example, sometimes "we schedule a test and then we have to postpone because of the system that is not or the internet is not working"(Mak-IT7). The problem is that ..." when it's not up and running, you can't do anything, and even students can't submit assignments" (RT_IT14). As a result, some lecturers have lost hope on the system, as they often have to find alternative solutions (such as resorting to paperwork and handwritten notes) when it is mal-functional (MN_IT22).

	Students	**Q**: Does the LMS always allow you to easily login, If NO, what challenges do you encounter? R: " It's not always easy, sometimes it takes time to login" (BNJ1) R: Ja, sometimes when you log in the internet, it is always down (BNJ2; DVD-2n1, MON2, MON3, MON11) R: "Not always, but most of the time" (BNJ3) R: "The only thing that is appearing is user account not allowed" (ABO 9) **Q**: How long does the LMS take to grant you access to the system? R: Ranging from 10 minutes to 40 minutes, the internet connection sometimes is very slow. (BNJ4; DVD-2n8) R: Maybe 2 minutes to connect sometimes is very slow (BNJ6; BNJ7; BNJ5) R: "Well it depends where you are and computer that you are using" (MON41; MON52) R: "is about 3 or 4 seconds " (DVD-2n 3) **Q:** Can you access the LMS when you are out of campus? R: "I've never really tried to use it off campus (BNJ8; BNJ9) R: "Yes" (DVD-2n2) **Q**: How many times can you attempt to login to the system? R: "Many times, I don't know"(BNJ14; BNJ18) R: "I've tried only 2" (DVD-2n 6) R: "Only about 5 times" (MON71) R: Its 3 times when the username and password has been incorrectly entered (DVD-2n5) **Q**: What are the causes of these access errors & problems? R: "sometimes it gives me an error that I'm still logged in and I'm at home already and it says I'm still logged in" (DVD-2n3) R: Tells you about incorrect password (DVD-2n4) R: The computer just freezes and the page freezes and then you just can't do anything (DVD-2n10; DVD-2n13, DVD-2n15)	**In terms of LMS user access by students, findings show that** apart from literacy issues, and physical access to the CPUT learning resources but the issue of easy access to login to the LMS is the main key to LMS usage at CPUT. The concern to most respondents is that the LMS is not always available and does not always allow students to easily login. In fact, students comments are "sometimes it takes time to login" (BNJ1); others claim that the university intranet is sometimes down (BNJ2; DVD-2n1); and at times the system blocks users with the message that says "user account not allowed" (ABO 9). However, duration it takes for the LMS to grant them an access various ranging from the minimum of 2 seconds, 2 minutes up to 40 minutes depending on the internet speed (DVD-2n 3; BNJ6; BNJ7; BNJ5; BNJ4; DVD-2n8). The issue of access does not only affect the access to the LMS page and duration it takes for the system to grant a user an access. It also expands to the place or area where students are accessing the LMS within the university premises. However, 2 students never tried to access the LMS outside campus (BNJ8; BNJ9), but there is one student who have tried (DVD-2n2). Regardless of where students access the LMS, findings report that some students attempt to login on the system "Only about 5 times" (MON71) whereas other students do not recall the number of times (BNJ14; BNJ18). Another student claims that he has only tried twice (DVD-2n 6) and another student advice that Its 3 times when the username and password has been incorrectly entered (DVD-2n5). However, one student declared that he tries the number of times to login due to error messages that he receives. For example, sometimes the system would give a message the "…I'm still logged in and I'm at home already and it says I'm still logged in" (DVD-2n3). With other students, it would give a password error message (DVD-2n4) or the computer and the page would just freeze to extent that they can't do anything(DVD-2n10; DVD-2n13, DVD-2n15)
	Network Administrator	**Q**: What are the criteria for one to have an access to the system? R: " When you register we've got stuff in place that automatically does that" (OF_NET36) R: "… we give them first account, account and password…" (OF_NET34) **Q**: How is the LMS access according to your understanding? R: "… and there were problems in the past, I think we've come a long way in stabilizing that environment…" (OF_NET61)	**In terms of LMS user criteria for network LMS access and usage, judgments by network administrator show that** for users to have an access to the system, they have go through certain criteria. When an administrator asked about the criteria used for first time user, he said, "we give them first account, account and password…" (OF_NET34). In fact, when users have the right to use the system, they still access LMS that is partially giving problems to its users (OF_NET61)