



**The effectiveness and the efficiency of the
electronic security system in the North-
West University, Mafikeng Campus**

D. P. Tabane



Orcid.org 0000-0003-4668-4930

Dissertation accepted in fulfilment of the requirements
for the degree *Master of Business Administration* at the
North-West University

Supervisor: Dr Seboka Kopung

Graduation ceremony April 2018

Student number: 16488407

DECLARATION OF ORIGINALITY

I, DIAU PHILEMON TABANE, declare that the mini-dissertation titled “ The effectiveness and efficiency of the electronic security system in the North-West University, Mafikeng Campus ,” submitted for the degree of Master of Business Administration at North West University, has not been previously submitted by me for a degree at this or any other University. This is my own work in design and execution and all material contained herein has been duly acknowledged.

CERTIFICATE OF ACCEPTANCE FOR EXAMINATION

This mini-dissertation titled “The effectiveness and efficiency of the electronic security system in the North-West University, Mafikeng Campus,” written by DIAU PHILEMON TABANE (student number 16488407) is hereby recommended for acceptance for examination.

Supervisor: Dr Seboka Kopung

Signature:_____

ACKNOWLEDGEMENT

In the designing and writing of this study, I received a lot of support from various people who were always encouraging me to carry on with my study even when it was tough. In particular I am forever grateful for my supervisor, Dr Seboka Kopung for his indispensable advice and guidance in the shaping and production of this work, above all the prayers he was offering throughout were very much fulfilling.

I am also grateful to the entire IT team and Protection Services team who were always providing support, giving me unending motivation, issuing out the necessary information which helped me out to carry on with the study. Their enthusiasm and warm encouragement made it possible for me to complete this study. Special thanks to my mother Tryphinah Tabane for the support and encouragement.

A special word of thanks to my friends and my children who have been helpful during the study, and finally to the Director of Protection Services Mr Aubrey Welken who always gave me moral support and encouragement to complete this study.

Above all, I wish to express my most sincere gratitude to the Almighty God for making everything possible and for the successful completion of this research.

ABSTRACT

The purpose of the study was to analyse the efficiency and effectiveness of the electronic security system at the North-West University, Mafikeng Campus. The main aim of the electronic security system is to provide, defence, protection and safety to the people and assets of the organization against intruders. The protection occurs on the outer and the inner perimeter of the property and by so doing efficient and effective electronic security system must be in place.

Electronic security plays a major role in the life of people and in protecting the assets of the organization. When the electronic security system is effective and efficient then the company becomes very successful in terms of the progress. In the outer perimeter which is the actual property lines, is to check and control who walks or drive onto the property without the concern of the owner. The two security concepts in the perimeter security are the natural security control and territorial reinforcement. In the natural access control, criminals like to feel being in control because of entering and exiting the area with the perception that the risk is very low and are unnoticed in the area.

The total population that took part in the analysis of the Electronic Security System consist of different categories; second and final year students doing computer science and information technology, and security personnel within the campus and private companies.

From the findings of the study, it was recommended that the University management should implement security measures in line with their respective security policies in order to mitigate identified risks. The management should have appropriate security solutions in place to protect university assets, students, employees and communication links against abuse or attacks. The responsiveness of the security system to threats is very much important to eliminate the vulnerabilities and threats beforehand and to avoid unnecessary costs against the university. The university should do everything in its power to provide an increased and improved service over time. Effective and efficient service delivery will bring about good and successful results, and that will make customers happy at the end of the day. The management should follow processes and procedures of the security act in order to ensure that the entire university is safe and secure.

Table of Contents

DECLARATION OF ORIGINALITY	i
CERTIFICATE OF ACCEPTANCE FOR EXAMINATION.....	ii
ACKNOWLEDGEMENT	iii
ABSTRACT	iv
LIST OF TABLES	ix
LIST OF TABLES	ix
ACRONYMS x	
CHAPTER ONE – STUDY OVERVIEW	1
1.1 INTRODUCTION	1
1.2 BACKGROUND	2
1.3 PROBLEM STATEMENT AND CORE RESEARCH QUESTIONS	3
1.4 RESEARCH OBJECTIVES	4
1.5 RESEARCH QUESTIONS.....	5
1.6 IMPORTANCE OF THE PROPOSED STUDY	5
1.7 DELIMITATION AND ASSUMPTIONS	6
1.8 RESEARCH ETHICS	6
1.9 DEFINITION OF KEY TERMS	7
1.9.1 Security	7
1.9.2 Electronic security system	7

1.9.3	Access control	7
1.9.4	Peripheral device	7
1.10	CHAPTERS LAYOUT	8
1.12	LINK WITH THE NEXT CHAPTER	9
	CHAPTER TWO – LITERATURE REVIEW	10
2.1	INTRODUCTION	10
2.2	ELECTRONIC SECURITY COMPONENTS	11
2.2.1	CCTV surveillance system	11
2.2.2	Fire detection and alarming system	12
2.2.3	Attendance and access control system	12
2.3	SECURITY RISK MANAGEMENT	13
2.3.1	Crime prevention	14
2.4	EFFICIENT ELECTRONIC SYSTEM IN PROVIDING BETTER SERVICE DELIVERY	16
2.5	ACCESSIBILITY AND VISIBILITY OF ELECTRONIC SECURITY TO PEOPLE	19
2.5.1	Vulnerability of the electronic security to attack	20
2.5.2	Asset management and access control	22
2.6	CONCLUSION	22
2.7	LINK WITH THE NEXT CHAPTER	22
	CHAPTER THREE - RESEARCH METHODOLOGY	23
3.1	INTRODUCTION	23

3.2	RESEARCH METHODOLOGY	23
3.2.1	Description of Overall Research Design	23
3.2.2	Population	24
3.2.3	Data Collection	24
3.2.4	Data Analysis.....	25
3.3	RESEARCH DESIGN	25
3.4	DATA COLLECTION	25
3.4.1.	Data collection procedure	26
3.5.	DATA ANALYSIS	26
3.6	VALIDITY AND RELIABILITY	26
3.7	LINK TO THE NEXT CHAPTER.....	27
	CHAPTER FOUR - DATA ANALYSIS	
	28	
4.1	INTRODUCTION	28
4.2	DATA INTERPRETATION	29
4.2.1	Biographic information	29
SECTION 2	35	
4.2.2	Impact of the electronic security system with regard to running business	35
SECTION 3	36	
4.2.3	Electronic security services.....	36
4.2.4	Factors affecting the use of electronic security system information	38
4.2.5	Information Quality	39
4.2.6	What services will you be interested in on the Electronic Security System	41

4.2.7	Service Delivery Output	43
4.3	LINK TO THE NEXT CHAPTER.....	45
CHAPTER FIVE - DISCUSSION, RECOMMENDATIONS AND CONCLUSIONS		
		46
5.1	INTRODUCTION	46
5.2	DISCUSSION	47
5.2.1	How to analyse the nature of the electronic security system during the student protest?	47
5.2.2	How to analyse the effectiveness of the electronic security system at the time of the protest?	48
5.2.3	How to analyse the efficiency of the security system in delivering the service?	48
5.2.4.	Which electronic security system will give best results for NWU Mafikeng campus?	49
5.2.5	What impact does the installed system have in a day to day running of the business?	49
5.3	RECOMMENDATIONS	49
5.4	CONCLUSION	50
5.5	AREAS FOR FUTURE RESEARCH	52
REFERENCE 53		
APPENDIXES		
		57
APPENDIX A– ETHNICAL CLEARANCES		
		57
APPENDIX B – LETTER OF EDITING		
		58
LIST OF TABLES		

Table 4-1 Biographical information	29
Table 4-2: Impact of the electronic security system with regards to running business	35
Table 4-3: How is the impact of the Electronic Security System with regard to crime	36
Table 4-4 Does the electronic security system provide the type of service the university requires?	37
Table 4-5 : Factors affecting the use of electronic security system information	38
Table 4-6: Information Quality	39
Table 4-7: What services will you be interest in on the Electronic Security	41
Table 4-8: Service Delivery Output	43

LIST OF FIGURES

Figure 4-1 : Gender Analysis	31
Figure 4-2: Age group analysis	32
Figure 4-3: Educational Level	33
Figure 4-4: Occupation	34

ACRONYMS

Acronyms	Meaning
ACS	Access Control System
BSS	Bosch Security System
CCTV	Closed Circuit Television
CPE	Customer Premise Equipment
CPS	Cyber Physical Security
CPTED	Crime Prevention Through Environmental Design
DoD	Dial on Demand
DTMS	Data Transmission Media System
DVR	Digital Video Recorder
ESS	Electronic Security System
FDS	Fire Detection System
IDS	Intrusion Detection System
IP	Internet Protocol
IT	Information Technology
NAC	Network Access Control
NVR	Network Video Recorder
NWU	North-West University
PS	Peripheral Devise
PTZ	Pan, Tilt, Zoom
REX	Request To Exit Devices

SRM	Security Risk management
TZAC	Trust Zone Access Control
UFC	Unified Facilities Criteria

CHAPTER ONE – STUDY OVERVIEW

1.1 INTRODUCTION

There are different types of security system, for an example the physical security system, electronic security system (ESS) and information security system to name a few. The physical security refers to the guard patrolling around the designated areas of concern, while electronic security system is the number of electronic devices connected together in a network to control the access to the property, to view and detect the movements of people and cars in the property, for example the access control system (ACS), closed circuit television (CCTV) and intrusion alarm.

The main focus was on the electronic security system therefore, physical security did not form part of the study. The main aim of the security is to provide defence, protection and safety to the people and assets of the organization against intruders. The protection will be done on the outer and the inner perimeter of the property and by so doing efficient and effective security system must in place.

In the outer perimeter which is the actual property lines, is to check and control who walks or drives onto the property without the concern of the owner. The two security concepts in the perimeter security are the natural security control and territorial reinforcement. In the natural access control, criminal like to feel being in control because of entering and exiting the area with the perception that the risk is very low and are unnoticed in the area.

According to Crowe and Fennelly (2011), the territorial reinforcement prevents unauthorized entry and creates a clear distinction between public and private property. The legitimate occupants of the property have the sense of ownership and will notice the people who are not part of the property or organization. The intruders will have the hard time to get access into the premises or property. The ultimate goal is to keep the intruders off the property. The inner perimeter security includes the door, windows and walls of the building. To protect the inner perimeter, locks, alarm systems and access control must be in place for security reason.

1.2 BACKGROUND

Electronic Security System is the protection resulting from all measures designed to deny unauthorized persons access to certain areas or to acquire information of value or to gain entry to some assets from the house or company. Haren, and Lai (2007) described the electronic security system as a series of integrated electronic devices working together with the central control panel to control and protect potential intruders. The definition of the electronic security system is found in its name, it is literally a means or method by which something is secured through a system of interworking components and devices.

Security services has grown significantly from years back to now due to technological advancement where now the electronic security system has relieved most of the work which was done by the physical security, Haren, and Lai (2007). All electronic security system work on the same basic principle of securing entry points, like gates, doors, windows and hidden places as well as interior space containing valuables. According to Hwang and Li, (2000) security is essential if we are to preserve privacy, promote business, and reduce criminal activity.

According to Pieprzyk, Hardjono, and Seberry (2013), “Enhancing security might have meant putting better locks on the front door. The essential functions of the secure system ensure that when the business is run, reliable operations with consistent uptime and without electronic disruptions or threats”. According to unified facilities criteria (UFC), electronic security systems, 2013, Electronic security systems (ESS) consist of access control systems (ACS) (card reader systems), closed-circuit television (CCTV) system, intrusion detection systems (IDS), data transmission media systems means to communicate information internally and externally to DoD (Dial on Demand) sites), and provision of local or regional dispatch centres (also known as security command centres).

Electronic security systems are one part of an overall physical security plan. Within the ESS there is a Control Panel which is the computer that arms and disarms the security systems, communicates with each installed components, sound the alarm when the security zone is breached and communicates with an alarm monitoring company.

Motion Sensor is the security components which when armed, protect a given space by creating an invisible zone that cannot be breached without sounding an alarm, these are typically used to protect rooms containing valuables, as well as areas less frequented in larger homes or companies. According to Compartmented (2013), the Surveillance Cameras (CCTV) available in both wired and wireless configurations, surveillance cameras can be used in several different ways as part of an overall security system, they can be used to record any security breaches, which could result in having footage of the property invasion, including good look at the burglars and perhaps even the vehicle they drive.

1.3 PROBLEM STATEMENT AND CORE RESEARCH QUESTIONS

South African Universities are facing enormous security challenges with the uprising of the 'fees must fall campaign'. North-West University is one of the Universities which suffered in terms of losing assets as a result of ineffectiveness and inefficiency due to the security system that existed at the time. North-West University, Mafikeng Campus has gone an extra mile to look for the company which can bring a better service to the Campus in terms of the Electronic Security System by advertising a tender.

Compcrete is the company which is rendering the service for the university in terms of installation and maintenance of the electronic security system. According to Redlich and Nemzow (2006), an adaptive method, system and program for securing data against a plurality of electronic and environmental events directed at computers utilizes a hacking monitor which generates attack warnings (such as a hacking warning) dependent upon the severity of the attack.

Fundamental question should now be posed. First, what measures can we take to make personal and professional assets a less attractive target? Second, how much security is enough? Simply put, can an attack on security be made so costly, so risky that it exceeds the value derived from the attack? Yes, it can be. And in doing so, we can stop some attacks before they start. Every aspect of the assets that presents an opponent an opportunity for attack can be classified as an attack surface.

The actions that can be taken to mitigate the consequences of the attack are classified as counter-measures. The objectives in designing a secure system are two-fold; to limit availability of attack surfaces and wherever we must expose an attack surface and to incorporate effective counter-measures to reduce attractiveness of the attack surface (Redlich & Nemzow, 2006).

The cost of an attack can be raised by raising the effort required to gain access (improved lock), escape the threat of physical harm, or avoid detection and prosecution (the alarm). So, when securing commercial products and services that is exactly what has to be done: raise the risk of mounting an attack. Moreover, reduce the likelihood that an attack, once mounted, will be successful and increase the probability that any attack, successful or not, will be detected.

1.4 RESEARCH OBJECTIVES

The main objective of the study is to analyse the efficiency and effectiveness of the electronic security system in the North-West University, Mafikeng Campus. With regard to the above stated problem, the following research questions will be addressed in this research project.

The main objective will be achieved through the following sub-objective which are;

- To analyse the nature of the electronic security system during the student protest.
- To analyse the effectiveness of the electronic security system at the time of the protest.
- To analyse the efficiency of the security system in delivering the services
- To ascertain if the electronic security system is the acceptable system to be used in an institution such as North-West University; and
- To analyse the impact of the electronic security system in the day to day running of the business.

1.5 RESEARCH QUESTIONS

- How to analyse the nature of the electronic security system during the student protest?
- How to analyse the effectiveness of the electronic security system at the time of the protest?
- How to analyse the efficiency of the security system in delivering the service?
- Which electronic security system will give best results for NWU Mafikeng campus?
- What impact does the installed system have in a day to day running of the business?

1.6 IMPORTANCE OF THE PROPOSED STUDY

According to Subashini and Kavitha (2011), numerous organizations without electronic security system, when compared to those with professionally monitored system, are more likely to be burglarised because burglars are opportunistic by nature and are on the hunt for easy target. Organizations without security system have high risk of attack. Advantage is the ability to remotely manage organization, with this, you can typically arm and disarm your security system from anywhere in the world via a web-enabled device, to monitor who arrives and leaves the premises.

Semertzidis, Dimitropoulos, Koutsia and Grammalidis (2010) stated that surveillance cameras are great for monitoring access points and unstaffed areas, which is important in providing a safe environment for employees, students and people who will be visiting the campus. ESS are there to reduce violence and harassment, creating healthier or conducive workplace.

Effective ESS can improve overall productivity and customer service. Broder and Tucker (2011), Electronic security system does not have inventory shrinkage and property damage, they are deterrents to crime and can help to lower liability and insurance costs. According to Norman (2011), the primary function of an ACS was to ensure that only authorized personnel are permitted ingress to a controlled area.

Norman (2011) believed that the ASC should log and archive all transactions and alert authorities of unauthorized entry attempts. An ACS can have many elements, including electric locks, card readers, biometric readers, door contacts, and request-to-exit devices, all monitored and controlled by a distributed processing system and one or more workstations.

1.7 DELIMATION AND ASSUMPTIONS

The scope of the study was just to analyse the effectiveness and efficiency of the electronic security system. The study focused on certain part of the electronic security system which is the Access Control System (ACS), Closed Circuit Television or Surveillance Cameras (CCTV), Intrusion Detection System (IDS), fire and smoke detectors and the way they impact on day to day running of the business.

If the Electronic Security system of the organization is effective and efficient, the production will be high because the values and the strategies of the organization will be achieved. In general, the Electronic Security System designer must balance security requirements with life safety, fire-alarm interface, and normal operational convenience factors. Physical security and Perimeter fence will not be part of the study for now because they do not form part of the Electronic Security Systems.

1.8 RESEARCH ETHICS

The information contained in this research does not pose any danger/harm to the respondents. The information will always be available and accessible for any use by the respondents. The respondents will be safe and highly protected, that means no response from respondents will be revealed or exposed, everything will be treated with high confidentiality. According to Haggerty (2004), the conclusion suggests that one effect of the increasingly formalized research ethics structure is to rupture the relationship between following the rules and acting ethically. The researcher adhered to the university ethical policy and sought ethical clearance before commencing with data collection.

1.9 DEFINITION OF KEY TERMS

(a) Security

According to the Bowers, Crowhurst, Alexander, Callaghan, Eales, Guy, McCann and Ryan (2002), security means the safety of the country, company or individual against espionage, theft or other danger or risk.

(b) Electronic security system

According to United States Corps of Engineers (2013), electronic Security System (ESS) is the integrated electronic system that encompasses the Access Control System (ACS), interior and exterior Intrusion Detection System (IDS), CCTV systems for assessment of alarm conditions, the DTM, alarm reporting systems for monitor, control, and display, and the policies, procedures, and response times that ensure that all elements of the ESS work effectively. It is part of an overall physical protection system.

(c) Access control

According to Introductory Guide Access Control by Example by Bosch Security System, (2009), access controller is an electronic device which handles input and output signals from and to the peripheral components (readers, door controllers, REX units, magnetic contacts etc.). It is an interface through which the access control software communicates with these components, but the controller is able to handle some signal events on its own if it temporarily loses its connection to the software.

(d) Peripheral device

According to Marianetti, and Hawkins (2003), peripheral device is a "device that is used to put information into or get information out of the computer.

There are three different types of peripherals:

- Input, used to interact with, or send data to the computer (mouse, keyboards.)
- Output, which provides output to the user from the computer (monitors printers.)
- Storage, which stores data processed by the computer (hard drives, flash drives.)

1.10 CHAPTERS LAYOUT

Chapter one looked at the overview of different types of security system and what each system entails and narrowed it down to the electronic security system (ESS), which is the area of concern. The chapter described and explained ESS to be the system which uses the electronic components connected together in a network for easy communication and security purposes, so that information can be stored and be retrieved when necessary. The chapter explained the importance of having functional and active ESS and the benefits thereof.

Chapter two focused mainly on the literature review that is specifically how other researchers viewed different aspects of the research topic under study and what other researchers found out what needs to be done.

Chapter three was about research Methodology, in this chapter the main focus was the collection of facts or data from other researchers. Research Methodology was a way to find out the result of a given problem on a specific matter or problem that was also referred as research problem. In Methodology, researcher used different criteria for solving/searching the given research problem. Different sources used different type of methods for solving the problem

Chapter four dealt with data Analysis, was analysing the data and interpretation of the analysis. This chapter dealt with the process of evaluating data using analytical and logical reasoning to examine each component of the data provided.

Chapter five details discussions, recommendations, conclusion and areas for future research. This chapter outlined the interpretations given by the researcher of the significance of the findings of a research project for the client's business, along with recommendations for action. These recommendations would be based on the research and on any other relevant information available to the researcher, including their own past experience in a market or in business.

1.12 LINK WITH THE NEXT CHAPTER

The next chapter which is chapter two, is the literature review which connect perfectly with chapter one. This chapter examined the reasons for the importance of the literature review, and the things which it tried to achieve. It also explored the main strategies which could be used to write a good literature review.

CHAPTER TWO – LITERATURE REVIEW

2.1 INTRODUCTION

According to Foodman (2005), electronic security system referred to any electronic equipment that could perform security operation like surveillance camera, access control, alarming or intrusion control to a facility or an area which uses power from mains and a power backup like battery. It also includes some of the operations such as electrical and mechanical gear.

Determination of a type of security system is purely based on area to be protected and its threats. Foodman (2005) showed that the system is important for many reasons including safeguarding the health and safety of employees, as well as serving as a protection for property and equipment and come in many designs and sizes. The system is always watching, listening, monitoring and recording everything that goes on in the facility.

Solutions have the knowledge and skill necessary to provide life safety and integrated security system to our clients based on their specific needs and environments. According to Krause (2006), the ESS is committed to achieving a safe and secure environment for employees and visitors while offering protection for information and property and help protect the things client care about and ensure satisfaction with the product, services and the entire process of conducting business.

Zittrain (2008) maintained that electronic security system relates to leveraging innovation in defensive holding by anticipating unapproved access to individuals and property. The government is a universal and major customer of such security administrations and business sections and also utilizes the security systems for their workers for giving security; one can also witness the usage of electronic security system in domestic application and small stores. Electronic security systems extensively comprise of alarms, access control and CCTV (closed-circuit television), which are prominently and broadly utilized.

The system is broadly utilized within corporate working places, commercial places, shopping centres and many more places. These systems are also used in railway station, public places and etc. These systems are also utilized as access control systems, fire recognition and avoidance record system. It is a known fact that the crime rates are increasing day by day so most of the people are usually not feeling comfortable until they are provided with a sure security, either be at the office or home (Zittrain, 2008).

According to Zittrain (2008), a better electronic system should be chosen for securing purpose. Classification of security system can be done in different ways based on functioning and technology usage, conditions of necessity accordingly. Based on categorizing electronic security system as follows:

- CCTV Surveillance Security System
- Fire Detection/ Alarming System
- Access Control/ Attendance System

2.2 ELECTRONIC SECURITY COMPONENTS

2.2.1 CCTV surveillance system

CCTV surveillance system is the process of watching over facility which is under suspicion or area to be secured and the main part of the surveillance electronic security system consists of camera or CCTV cameras which forms eyes to surveillance system. Surette (2005) showed that the system consists of different kind of equipment which helps in visualizing and saving of recorded surveillance data. CCTV is a system that allows you to see what's happening no matter where you are.

System consists of different kinds of equipment which helps in visualizing and saving of recorded surveillance data. Surette (2005) showed that the main feature of this system is that, it can be used at any places where we watch the human being in action. CCTV surveillance systems include cameras, network equipment's, IP cameras and monitors.

The alarm rings after receiving the signal from the cameras which are connected to CCTV system which are concerned with the detection of interruption or suspicion occurrence on the protected area or capability, the complete operation is based on the CCTV surveillance system through internet.

2.2.2 Fire detection and alarming system

Fire detection and alarm system can also be referred as a detection and alarming system as it gives an alarming alert to concern on detection of interruption or suspicion happening on a protected area or facility. System generally consists of detector using a sensor followed by an alarm or an alerting circuit. According to Bhattacharjee, Roy, Ghosh, Misra, and Obaidat (2012), the main function of this system is to rapidly extinguish an advancing fire and alarm tenants preceding impressive harm happens by filling the secured zone with a gas or concoction smothering operator. These systems provide a strong deterrent to burglars and employee theft.

2.2.3 Attendance and access control system

Saparkhojayev and Guvercin (2012) showed that the system which provides a secured access to a facility or another system to enter or control it can be called as an access control system. According to the user credentials and possessions access control system is classified, what a user uses for access makes system different, user can provide different types like pin credentials, biometrics or smart card. An advantage of this type of system is that it can help safeguard against workplace violence.

The researcher made use of different sources to analyse the effectiveness and the efficiency of the electronic security in different organizations both locally and internationally. The main purpose of security system is to achieve the maximum cost effectiveness and most efficient possible business benefit. According to Saparkhojayev and Guvercin (2012), the most significant benefit of installing a security system revolves around the concept of future proofing.

Sajkowsky (2006) stated that the security system also provides the opportunity to regularly analyse the security requirements of the facility or set of facilities. If we imagine a commercial office building, the security manager might require the installation of access control, intruder detection and video surveillance system. According to Saparkhojayev and Guvercin (2012) the security system therefore allows the end-user to minimize the cost of an upgrade to meet any developments in the security requirements. Therefore, the effectiveness and the efficiency of the electronic security system must be of the most significance in the organization and it is much more important to check how other people viewed it on different aspects of security

2.3 SECURITY RISK MANAGEMENT

Security Risk must be taken into consideration and the ways of mitigating those risks in order to combat crime and prevent loss of assets. According to Paris (2013) Security Assessment Report and Recommendations; safety and security programming in an academic setting is a delicate balance of responses to and preparation for potential risks.

According to Paris (2013), Criminal or other aberrant activities, College and community emergencies, and existing organizational mission and culture, as well as cost and perceived need, are all elements of importance. A “systems” approach that includes the application of security and safety technologies and appropriate policies and procedures, as well as the assignment of individual and organizational responsibilities to various personnel and entities, is required if this effort is to be successful.

Safety and security programming efforts need to be consistent with the risks inherent in its campus environments and with the College’s mission. Paris (2013) showed that the key to successful safety and security programming is a viable technology infrastructure, the development and implementation of an appropriate philosophy and policies, the support of key College administrators, and the empowerment of professionally trained, properly equipped personnel.

Efforts to determine the College’s current level of preparedness were based on the premise that effective programming requires an understanding of risks and the balancing of critical elements. Paris (2013) showed that the application and integration of these four elements varies at every institution based on the risks identified, the risk tolerance of the administration and members of the community for various threats, real or perceived, available resources and capabilities, as well as other factors.

According to Nazareth and Choi, (2015), some institutions may rely more on technology than staffing. Others might employ robust, comprehensive policies and procedures focused on decentralized organizational responsibility rather than centralized program management, while still others might use extensive security staffs in various roles.

In a research study conducted by Olckers (2007), security risk management approach was applied to the findings in order to assess the risk (impact of crime) on either the absence of non-compliance to installed security measures so that recommendations (advice) could be formulated for the implementation of supplementary or additional security measures at the residences that had been victims of burglary.

2.3.1 Crime prevention

Crime Prevention is very much important because the organization will run smoothly without loss, and it will achieve its mission and vision, it will attract more clients or customers. According to Paris (2013), the campus has built environment provides many opportunities to improve safety and security by employing in both design and application various principles identified as Crime Prevention through Environmental Design.

While use in practice has existed for many years, indeed decades, the relationship between the application of Crime Prevention through Environmental Design (CPTED) principles and safety was not realized or studied until more recently. Paris, (2013) showed that Crime Prevention through Environmental Design (CPTED) is the concept of using the designed and built environment to create safe, visually open spaces and effective people flow or access controls.

Paris (2013) showed that it is accomplished through the creation of: Natural Surveillance - Natural surveillance is a design concept directed primarily at keeping possible intruders under observation and giving potential witnesses a clear view of activities in the defined spaces. It utilizes design features that may include window positioning, interior and exterior lighting placement and quality, and landscaping features and placement to increase the visibility of a property or building so that suspicious or improper behaviour might be seen and reported.

Paris (2013) showed that with appropriate natural surveillance, the opportunity to detect crime is enhanced by making the offender's behaviour more easily noticeable. Such observation might be by building occupants, pedestrians or passing security or police patrols. Students and property are safer when both may be observed by possible witnesses. Providing a good visual connection between academic facilities and public environments such as streets, walkways, and parking areas enhances campus safety (Paris, 2013).

Natural Access Control effectively uses defined walkways, lighting, fencing or other physical barriers, gates, way finding signage and landscaping to clearly guide appropriate people and vehicle movement. . Paris (2013) stated that the concept's primary purpose is to deny access to a potential crime target and creates a perception by the possible offender that there is risk in proceeding.

Various other means of access control such as locks, bars, or alarms may be helpful as a supplement to these natural access control measures. The appropriate design of facilities and spaces may also promote the perception of risk by potential offenders. Norman (2016); stated that the first measure of the effectiveness of a countermeasure is functional effectiveness. As each countermeasure has one or more functions as outlined below, one can estimate the ability to perform each function on a scale of 0 to 10, with 10 being absolute effective-ness and 0 being no function. The functions again include amongst others the Access control, Deterrence, Detection, Assessment, Delay, Response, and Evidence

Olckers (2007) looked at ways of Crime Prevention and said; " the outcomes focussed on providing security solutions in order to manage security crime risks such as residential burglary and that adhere to the principles of determining the best and most cost effective way of implementing and choosing a security system; enhancing the security system's deterrence factor; improving the security system's detection capabilities, enhancing the ability of the security system to delay a threat and developing efficiency by regular use, continual upgrading, provision of effective training, and having constant maintenance in place.

2.4 EFFICIENT ELECTRONIC SYSTEM IN PROVIDING BETTER SERVICE DELIVERY

Electronic security system refers to any electronic equipment that could perform security operations like surveillance camera, access control, alarming or an intrusion control to a facility or an area which uses a power from main. According to Subashini and Kavitha (2011), as the crime rates are increasing day by day so most of the people are usually not feeling comfort until good security either at the office or home therefore better electronic system must be chosen for securing purposes.

Sennewald, & Baillie (2015) stated that, Biometric based authentication and identification systems are the new solutions to address the issues of security and privacy. Using biometrics for identification restrict individuals from access to physical spaces and electronic services, an effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans.

Biometric technology is one area that no segment of the IT industry can afford to ignore. Biometrics provides security benefits across the spectrum, from IT vendors to end users, and from security system developers to security system users. According to Chen, Liu and Chen (2011), all these industry sectors must evaluate the costs and benefits of implementing such security measures.

According to Fatima (2015), different technologies may be appropriate for different applications, depending on perceived user profiles, the need to interface with other systems or databases, environmental conditions, and a host of other application-specific parameters. Its benefits can be summarized in the following points:

- Greater security—biometrics link a person to an action.
- Convenience—clients have no identification number or password to remember.
- Local verification—clients hold their identity information (e.g., on a Smart Card), so there is no need to verify identity via a central repository or server.
- Verification is swift and does not require staff.
- User identity is stored safely and is tamper-free.

However, Fatima (2015) maintained that the goal of any access control system is to let authorized people into specific places. Only with the use of a biometric device can this goal be achieved. A card-based access system can control the access of authorized pieces of plastic, but not who is in possession of the card. Systems using PINs (personal identification numbers) require that an individual only know a specific number to gain entry, (Fatima, 2015).

Who actually enters the code cannot be determined. Biometric devices verify who a person is by what they are, whether it be their hand, eye, fingerprint or voice. Biometrics also can eliminate the need for cards. Fatima (2015) showed that while dramatic price reductions have lowered the initial cost of the cards in recent years, the true benefit of eliminating them is realized through a reduced administrative effort.

A lost card must be replaced and reissued by someone. There is a cost associated with the time spent to complete the task. Eyes and hands are seldom lost, stolen or forgotten.

They also don't wear out and need to be replaced. Bye, Paczkowski, Parsel, Persson, Schlesener, and Shipley, Sprint Communications, (2015) found a way of strengthening security by a method of communicating with a computing device having a trusted security zone comprises mapping an identifier for a computing device with a trust zone access control (TZAC) address, composing a message comprising the trust zone access control address, and routing the message to the computing device based on the identifier. The computing device comprises a normal security zone and a trusted security zone that is separate from the normal security zone, and the trust zone access control address is a unique identifier associated with a hardware component of the trusted security zone within the computing device.

The message is internally routed to the trusted security zone within the computing device using on the trust zone access control address. In an embodiment, a method of communicating over a network comprises receiving a message at a computing device, internally providing the message to the trusted security zone based on the trust zone access control address and processing the message within the trusted security zone (Bye *et al*, | 2015).

The message comprises a routing address and a trust zone access control address, and the routing address comprises information configured to route the message to the computing device. The trust zone access control address is a unique identifier associated with a hardware component of a trusted security zone within the computing device.

Ryder (2016); stated that better service delivery could be achieved with the increased availability of high speed Internet connections, many devices have the ability to connect to remote services or sources. In addition, as the cost of high speed Internet connections decreases, many users may maintain a constant or near constant connection to the Internet.

Furthermore, as wireless communications systems expand, users can connect to remote sources at many different locations, including far from the user's work, home or other areas where the user typically can access the Internet. For example, wireless communications networks have expanded to the point where a device can connect to the Internet on a mountaintop in nature (e.g., while skiing or hiking), (Ryder, 2016).

Because of the enhanced ability of devices to connect to the Internet as a user moves or travels, a user can make an increased use of remote storage. In particular, a user can store information in one or more remote locations, while knowing that the information can remain accessible so long as the user has an Internet connection available.

This can allow a user to expand the amount of storage available to the user beyond the actual storage within the device (e.g., the storage of a hard drive or solid state drive in a device). A device can connect to any suitable remote storage source to store or access content. In some embodiments, one or more cloud storage solutions can be available to a user.

Evans (2005) stated that skills also impact on the service delivery by saying; the divide between the computer literate and the non-literate tends to perpetuate divides in income and education because without computer skills it is difficult to compete in the employment market. The international ramifications of this divide are severe and tend to

be compounded by the existing state of literacy and political and economic stability, as well as technical infrastructure.

Countries that find themselves on the wrong side of the divide will most likely find the divide increasing. Evans (2005) showed that the implications for economic and defence policy are immense. This creates a vacuum in power and an unstable situation that should be avoided at all costs. It is imperative to minimize the digital divide by promoting education through every avenue possible.

2.5 ACCESSIBILITY AND VISIBILITY OF ELECTRONIC SECURITY TO PEOPLE

Electronic Security System must be in the secure and safe place to avoid been tempered by people, the cables must be run in the hidden places. According to Shen, Everitt, & Ryall (2003), the essential components like the recording components (DVR/ NVR) and controller for access control, fire detection and smoke detection should be put in the safe and lockable room for protection of information, so that the information can be easily retrieved when needed. The system must not be difficult to be used by the end user.

According to Brodsky (2016), stated that potential vulnerabilities in control systems are exacerbated by insecure connections either within the corporate enterprise network or external to the enterprise or controlling station. According to Hyatt Jr, Trent, and Hall, (1998), organizations often leave access links open for remote diagnostics, maintenance, and examination of system status. such links may not be protected with any authentication or encryption (or if any exist, are considered rather weak as the individuals who configured the control systems environments wanted something easy to remember, since often times they had to maintain and manage hundreds of similar devices throughout a given area of region).

This increases the risk that an attempted external penetration could use these insecure connections to break into remotely controlled systems. According to Brodsky (2016,) some control systems use wireless communications systems, which are especially vulnerable to attack or leased lines that pass through commercial telecommunications facilities in either situation, the method of communications performs no security

methodologies whatsoever and if there are any security measures implemented, they are capable of being easily compromised.

Without encryption to protect data as it follows through these insecure connections or authentication mechanisms to limit access, there is limited protection for the integrity of the information being transmitted, and the process may be subjected to interception, monitoring of data from interception, and (eventually) penetration, (Brodskey 2016)

2.5.1 Vulnerability of the electronic security to attack

Shirlen and Hofmann, (2014) highlighted the vulnerability with regard to attack of the system that; entities or individuals with intend to disrupt service may use one or more of the following threat vector methods, which may be successful in their attack of control system:

- Disrupting the operation of control system by delaying or blocking the flow of information through the networks supporting the control system thereby denying availability of the networks to control systems operators and production control managers.
- Attempting to or succeeding in making unauthorised changes to programmed instructions within controllers, change alarm thresholds, or issue unauthorised commands to control station equipment, which could potentially result in damage to equipment, premature shutdown of processes (shutting down transmission lines or causing cascading termination of service to the electrical grid), or disabling control station equipment.
- Sending falsified information to the control system operators, either to disguise unauthorised changes or to initiate inappropriate actions to be taken by system operator, that is falsified information is sent or displayed back to system operators who may think that an alarmed condition has been triggered, resulting in system operators acting on the falsified information, thus potentially causing the actual event.

Redlich and Nemzow (2006) had this to say with regard to vulnerability of Electronic Security System to attack; managers can elect to counter a wide variety of security threats that are present with several strategies including detection, deterrence, vulnerability reduction, education and training. Clearly, a portfolio of strategies is preferred over the adoption of a single solution.

According to Redlich, *et al*, (2006), each security strategy entails different costs, effectiveness, and potential benefits; many of these are difficult to quantify. The business value derived from information security investment, although undeniable, may be difficult to estimate. This difficulty arises because of the uncertainties of threat manifestation, the extent of damage incurred, the ability to recover from successful attacks, any ripple effects to other parts of the business affected by a successful attack, and a loss of reputation,

Many factors affect these assessments, including innate vulnerabilities, the perceived attractiveness of targets (both organization and individual application), the number and sophistication of attackers, the availability of attack tools and vectors, and the extent and nature of backup facilities. Clearly, assembling an accurate business case can prove challenging.

Nonetheless, information security managers need to select security strategies on a periodic basis. In the absence of adequate tools to support these decisions, managers will speculate about whether the decisions that were made were appropriate for the task. A model that captures the complexities of the security decision while permitting the systematic exploration of alternative security decisions would be an invaluable aid to managers.

Using the design science research methodology this paper develops a model that allows information security managers to examine the effects of alternative security decisions on the organization's information assets. Given the need to capture the dynamic and fluid nature of the problem and to revisit the decision on a periodic basis, system dynamics is chosen as the modelling environment.

2.5.2 Asset management and access control

DiMase, Collier, Heffner, and Linkov (2015) stated that asset management and access control manages critical assets in the system that exhibit potential to introduce vulnerability through a functional role in the cps operating environment where interaction with the cps is required, it provides systems for an inventory of critical assets maintained by monitored access using verification credentials. This includes management of information relevant to the operation of the asset (e.g., software revision, firmware revision) and the process of granting or denying specific requests such for obtaining and using information and related information processing services; and to enter specific physical facilities (committee on nationals).

2.6 CONCLUSION

The literature review indicated that the efficient and effective electronic security system gave rise to the good service delivery which impact positively to the growth of the business and ultimately improves customer services.

2.7 LINK WITH THE NEXT CHAPTER

The following chapter (Chapter Three) provides the research design of the study indicating how data was collected and analysed

CHAPTER THREE - RESEARCH METHODOLOGY

3.1 INTRODUCTION

This chapter was about the research methodology applied to determine and analyse the effectiveness and the efficiency of the ESS in NWU, Mafikeng campus. The aim of the study was to discover answers to questions by the application of the scientific procedures. Furthermore, the intention of the study was to extract more information which was hidden, therefore, in this chapter facts or data were collected, analysed and conclusions drawn in the form of solutions to the problem identified.

3.2 RESEARCH METHODOLOGY

This chapter of the study was about the methodology applied to analyse the effectiveness and efficiencies of the electronic security system to reduce crime. The methodology in this research consisted of three steps namely literature survey, data source, study variables and methods of analysis. The intention of this chapter was to outline the importance of the research. Electronic security plays major role in the life of people and in protecting the assets of the organization. When the electronic security system is effective and efficient then the company becomes very successful in terms of the progress.

3.2.1 Description of Overall Research Design

Design is a process of making decisions before the situation arises in which the decision has to be carried out. It is the process of deliberate anticipation directed towards bringing an expected situation under control. Research entails two major stages: one is the stage of planning, and other is the stage of execution.

According to Creswell (2013), there are different forms of design, which are: qualitative, quantitative and mixed method. Some focus on the process on the collection of data only, while others extend their boundaries to cover data analysis. Research design is a wider context covering all aspects of research from the selection to the publication of the data. The study was quantitative analysis because according to Veres, Gray, Michel, Shen and Aiden (2011), this approach rarely enables precise measurement of the underlying phenomena.

3.2.2 Population

According to Gerstner (2006), population is a group of any species of organisms living in a specific region or ecosystem. All elements, individuals, or units that meet the selection criteria for a group to be studied. Gerstner (2006) shows that population is all elements, individuals, or units that meet the selection criteria for a group to be studied, and from which a representative sample is taken for detailed examination.

The total Population which took part in the analysis of the Electronic Security System consists of different categories; second and final year students doing computer science and information technology, and security personnel within the campus and private companies. The total number of the population who will be taking part is 35.

3.2.3 Data Collection

Questionnaires are probably one of the most widely used instruments to collect data in research. A questionnaire is a printed list of questions which respondents are asked to answer. Questionnaires are the most widely used instruments in this research to collect data in Survey research because they investigate attitudes and opinions that are not easy to observe and gives clear instructions (Collins, 2008: 17).

Data is appropriate if it is relevant, accurate, and entered without errors, timely, current, and kept up-to-date, secure, protected from deliberate and accidental damage or loss. Collins (2008:17) believed that there are a variety of ways in which one can collect data for research. If one applies a quantitative methodology one will typically emphasize meaning and experiences related to the phenomena.

3.2.4 Data Analysis

According to Enders (2010), data analysis is a process for obtaining raw data and converting it into information useful for decision making by users. Data is collected and analyzed to answer questions, test hypothesis or disprove theories. A pie chart was

used to display data graphically for ease of analysis, because pie charts are generally used to show percentage or proportional data usually the percentage represented by each category is provided next to the corresponding slice of pie (Enders, 2011).

Data analysis is the collecting and organizing of data so that a researcher can come to a conclusion. According to Boellaard (2009), quantitative data analysis is increasingly being recognized as an important tool for diagnosis, determination of prognosis, and response monitoring in oncology.

3.3 RESEARCH DESIGN

According to Lewis (2015), design is a process of making decisions before the situation arises in which the decision has to be carried out. It is the process of deliberate anticipation directed towards bringing an expected situation under control. Research entails two major stages: one is the stage of planning, and other is the stage of execution.

There are many forms of design. Some focus on the process on the collection of data only, while others extend their boundaries to cover data analysis. Lewis (2015) showed that Research design is a wider context covering all aspects of research from the selection to the publication of the data.

3.4 DATA COLLECTION

Johnson and Turner (2003) indicated that Questionnaires are probably one of the most widely used instruments to collect data in survey research. A questionnaire is a printed list of questions which respondents are asked to answer. Questionnaires are the most widely used instruments to collect data in Survey research because they investigate attitudes and opinions that are not easy to observe and gives clear instructions.

3.4.1. Data collection procedure

According to data collection is the process of gathering and measuring information on targeted variables in an established systematic fashion, which then enables one to answer relevant questions and evaluate outcomes. The following two data collection procedures are the most useful in the study, namely

- a) Primary data collection with focus Group Discussions and observations
- b) Secondary Data Collection where collecting data from documents, records and reports of others.

3.5. DATA ANALYSIS

This part of the study encompassed the analysis of data which was obtained from the statistical package known SPSS which was acquired from Statssa, Therefore, chapter four of this study would use tables, graphs and charts to demonstrate the effectiveness and efficiency of the electronic security system in the North West University, Mafikeng campus

Data analysis is a process for obtaining raw data and converting it into information useful for decision making by users. Data is collected and analyzed to answer questions, test hypothesis or disprove theories. The technique which will be used to analyze data will be a pie chart, because pie charts are generally used to show percentage or proportional data usually the percentage represented by each category is provided next to the corresponding slice of pie. The pie chart shows the percentage of different categories of participants in the study with regards to gender, age, education and occupation.

3.6 VALIDITY AND RELIABILITY

Reliability is the consistency of measurement or stability of measurement over the variety of conditions in which basically the same results should be obtained and validity is concerned with the meaningfulness of research components. According to Curtis (2011)

“Social Research, A practical introduction”, reliability refers to the extent to which the analysis of data yields results that can be repeated or reproduced at different times or by different researchers.

Validity refers to the extent to which truth-claims can be made, based on the research- it is dependent on the research measuring the appropriate phenomenon. Representative

Reliability is a relevant one because it is the reliability across sub-populations or groups of people and with validity, the construct validity is the one to take because it is based on logical relationship among variables, if the measure is valid, various indicators must operate in a consistent manner (Curtis, 2011).

According to Curtis (2011) Reliability will be used because researcher uses multiple indicators e.g. several items in a questionnaire all measure the same construct. Construct Validity is the ideal one to be used because it is based on the logical relationship among variables, if the measure is valid, various indicators must operate in a consistent manner.

3.7 LINK TO THE NEXT CHAPTER

This chapter outlined the process used to collect information and data for the purpose of making business decisions. The next chapter (Chapter Four) depend largely on chapter three because it analyses the collected information which has been dealt with from chapter three.

CHAPTER FOUR - DATA ANALYSIS

4.1 INTRODUCTION

This chapter provided analysis of the responses gathered from the NWU community. The study sought to identify factors contributing to the effectiveness and efficiency of the electronic security system in the university. The Electronic Security System is used for crime prevention and to protect assets and people. This system consists of access control system (ACS), closed circuit camera (CCTV), intrusion detection system (IDS) and many more.

The responses were collected using structured questionnaires administered by the researcher to the university community. The researcher presented and analysed the responses with a view of addressing the study objectives and also answering the questions outlined. In particular, the study aimed at addressing the following objectives:

- To analyse the nature of the electronic security system during the student protest.
- To analyse the effectiveness of the electronic security system at the time of the protest.
- To analyse the efficiency of the security system in delivering the services.
- To ascertain if the electronic security system is the acceptable system to be used in an institution such as North-West University; and
- To analyse the impact of the electronic security system in the day to day running of the business.

SPSS version 23 was used to analyse quantitative responses. A total of 35 questionnaires were distributed and a simple random sampling method was used to select the respondents. Of the 35 questionnaires handed out, 30 were returned forming a responses rate of 86%. This is a good response and conforms to recommendations by Bless *et al.* (2006)¹.

¹ Bless, C.; Higson-Smith, C. and Kagee, A. 2006. Fundamentals of social research methods: An African perspective. Cape Town: Juta and Company Ltd.

4.2 DATA INTERPRETATION

4.2.1 Biographic information

Table 4-1 Biographical information

Variable	Category	Responses	
		N	%
Gender	Male	12	40.0
	Female	18	60.0
Age group categories	20 - 30 yrs	8	26.6
	31 - 40 yrs	11	36.7
	41 - 50 yrs	9	29.9
	51 - 60 yrs	1	3.3
	61+ yrs	1	3.3
Educational Level	Matric	7	23.3
	Diploma	6	20.0
	Degree	10	33.3
	Masters	6	20.0
	PhD	1	3.3
Variable	Category	Responses	
		N	%
Occupation/ employment	Government employee	1	3.3

	Private Sector	11	36.7
	Self Employed	1	3.3
	Academic	4	13.3
	Students	13	43.3

According to the results presented in Table 4.1, respondents were fairly represented in terms of age and gender. Among the 30 respondents, 40.0% represented the males and the major part of the responses were provided by females forming a response rate of 60.0%. Likewise, there is also fair representation as far as their education and occupation is concerned.

The majority of the respondents have degree (33.3%) and masters (20.0%) as expected since the study was conducted at the institution of higher learning. It is also worth noting that during the study period, not only students and staff members took part in the study. There were people from other institutions such as government (3.3%) and the private sectors (36.7%).

PIE CHART 1: GENDER

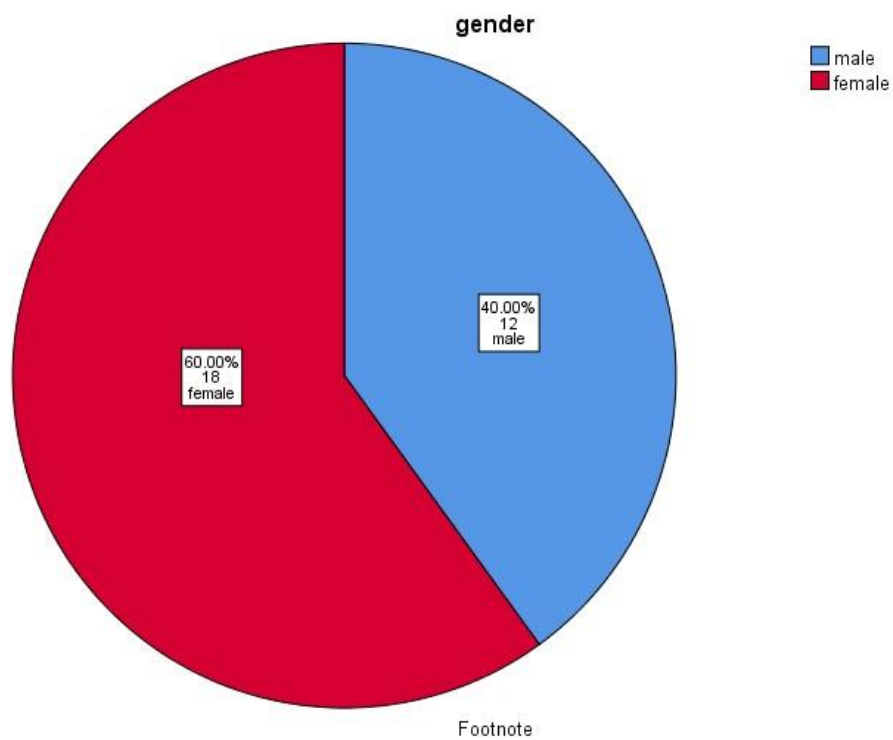
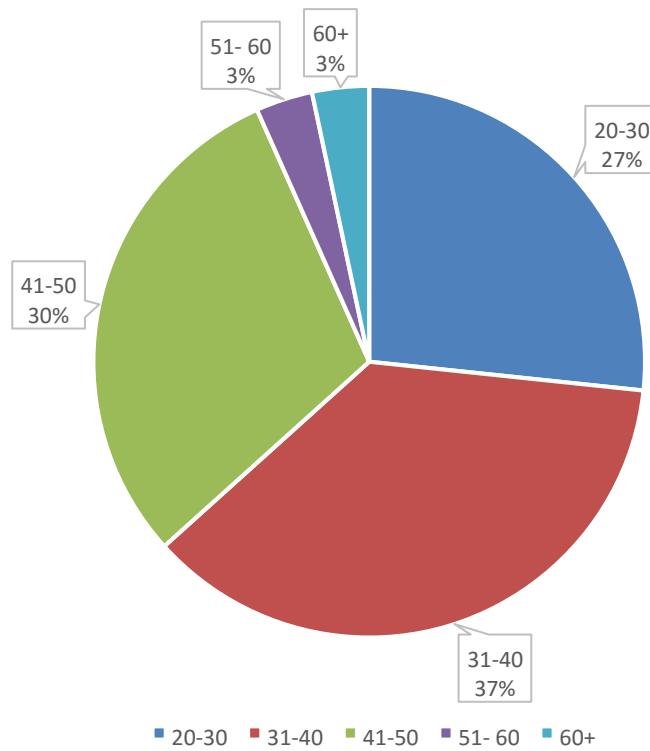


Figure 4-1 : Gender Analysis

Figure 4-1 shows 60.0% of females' participants and 40.0% males' participants in the study.

PIE CHART 2: AGE GROUP



Age Analysis

Figure 4-2: Age group analysis

The pie chart in Figure 4-2 shows different age categories of participants. The knowledge base is still concentrated between ages 31 and 61 plus.

PIE CHART 3: EDUCATIONAL LEVEL

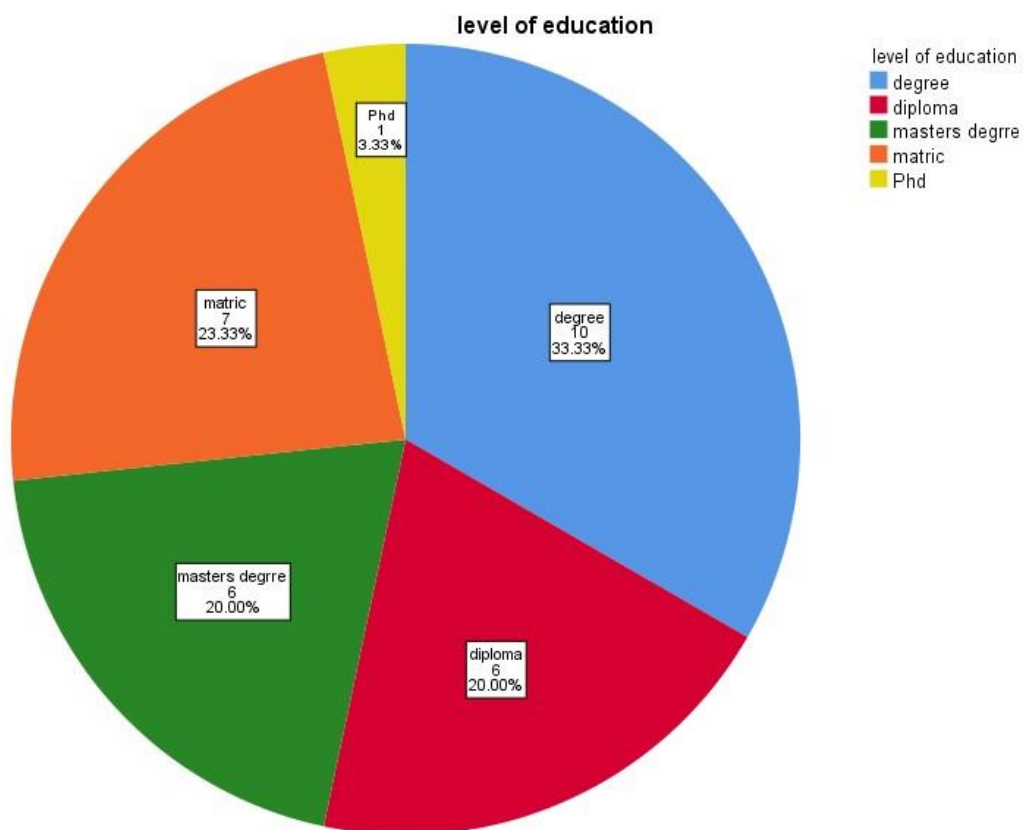


Figure 4-3: Educational Level

Figure 4-3 shows the level of education of all the participants who took part in the study.

PIE CHART 4: OCCUPATION

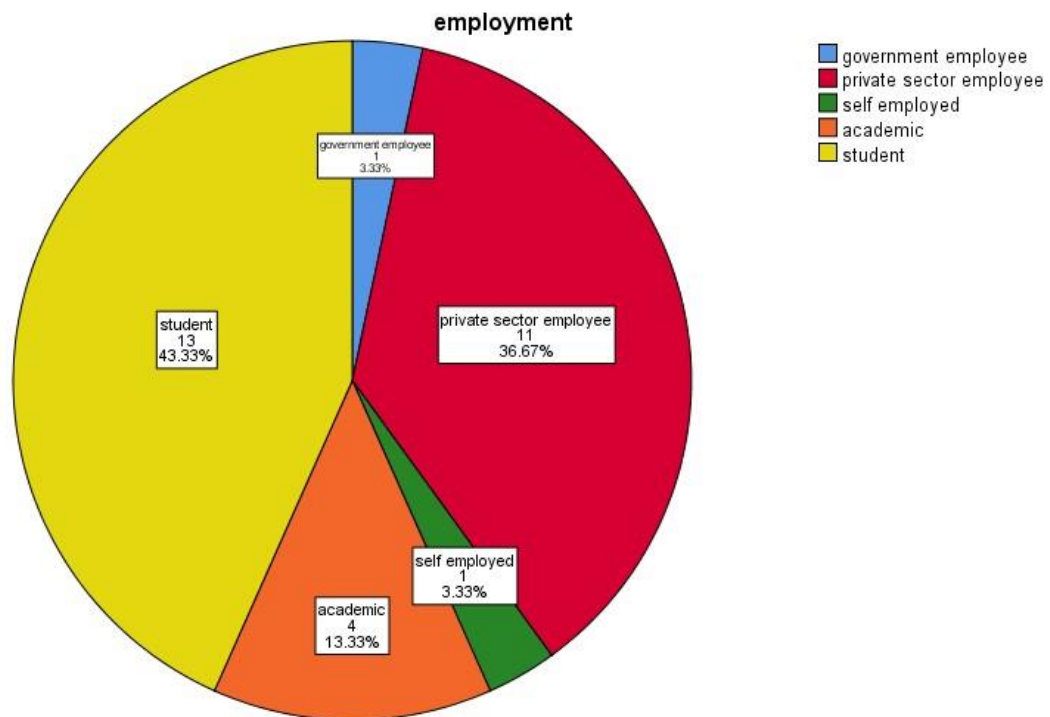


Figure 4-4: Occupation

Figure 4.4 shows the occupation or employment of all the participants who took part in the study.

SECTION 2

4.2.2 Impact of the electronic security system on running business

Table 4-2: Impact of the electronic security system with regards to running business

Question	Yes	No
Is the system suitable for the particular business/organisation?	24 (80.0%)	6 (20.0%)
Does the system actually meet the needs of the business/organisation?	25 (83.3%)	5 (16.7%)

Does the electronic security system need any improvement?	23 (76.7%)	7 (23.3%)
Is the electronic security system user friendly?	23 (76.7%)	7 (23.3%)
Does the electronic security system operate quickly, smoothly and with minimal waste?	23 (76.7%)	7 (23.3%)
Can an intruder gain unauthorised access to critical resources?	21 (70.0%)	9 (30.0%)
Are the electronic security components easily accessible?	29 (96.7%)	1 (3.3%)

As far as the impact of electronic system with regard to the running business was concerned, in Figure 2, most of the respondents were strongly in agreement (96.7%) about the ease of access to electronic security components followed by those who also concurred that the system actually meet the needs of the business (83.3%) and the suitability of the system for the operation of the business (80%).

About 76.7% of respondents were equally on the same page about the quick and smooth operation of electronic security system with minimal waste, its user-friendliness, and need for improvement. A worrisome fact concerning unauthorised access to critical resources gained by an intruder (70%). This could be a food for thought and may need an attention.

SECTION 3

4.2.3 Electronic security services

Table 4-3: impact of the Electronic Security System with regard to crime

How is the impact of the Electronic Security System with regard to crime?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Reliable	20	66.7	66.7	66.7
	Unreliable	10	33.3	33.3	100.0
	Total	30	100.0	100.0	

The impact of the Electronic Security system with regard to crime means that the type of security system installed at the university can reduce any disruption of the daily functions/ services of the university or can be the cause of the occurrence of human life and health hazards. This research document discusses the impact of electronic security system, the electronic component of the field on the process of the operation of the crime prevention.

The system should show maximum reliability and safety to the university. Table 4.3 showed clearly that 66.7% of the respondents believe and agree that the effect/impact of electronic security system to crime is positive, meaning the system is reliable, it can help to reduce crime and ensures safety in the campus. While 33.3 of the respondents totally disagree with the fact that electronic security system is reliable and can help reduce crime in the campus.

Electronic security system components form set of elements that operate together in order to achieve the assumed level of security, and are connected together to achieve certain objective that is mainly protection and crime alleviation in the campus. The use of system should greatly reduce the risk of malicious attack and damage by denying unauthorized access and be reliable to customers.

Table 4-4 Does the electronic security system provide the type of service the university requires?

Does the electronic security system provide the type of service the university requires?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	16	53.3	53.3	53.3
	No	14	46.7	46.7	100.0
	Total	30	100.0	100.0	

Vulnerability management, security measures, capabilities and access control, hardware protection, secure operating system, easy identification of suspects, good and clear visuals of footages, secure and protected environment are the most services that the university require in order to operate efficiently and effectively with minimal disturbance. To be able to access information, systems, and business processes, people and assets must be managed and controlled on the basis of business and security requirements.

Access to, or from, internal and external networks and network services must be managed and controlled. Security requirements and services must be assessed, identified, documented, and agreed at all times, therefore the system installed should provide the type of services the university requires. The purpose of the electronic Security System in the university is to reduce the risk of theft, fraud or misuse of assets.

In the Table 4.4, 53,3% of respondents said yes to the fact that the electronic security system provided the type of service the university required. This meant that the services offered by the Electronic Security System was most satisfying. The 46.7% of the respondents gave a the different story by saying services given by the Electronic Security Services were not of good quality therefore, they said no to the type of service offered.

4.2.4. Factors affecting the use of electronic security system information

Table 4-5: Factors affecting the use of electronic security system information

	N	Min	Max	Mean	Std. Deviation	Skewness
Electronic Security System is easy to use.	30	1	5	3.73	1.112	-1.041
Electronic Security System provides prompt service	30	2	5	3.70	1.055	-.287
I find it easy to gain access to anywhere I want to go.	30	2	5	3.77	.971	-.462
Using Electronic security system preserves public's perception of brand strength or organizational reputation.	30	2	5	3.70	.915	-.208
Electronic Security System prevents legal action by providing good service.	30	2	5	3.70	.837	-.500

According to the respondents' views concerning system quality presented in Table 4.5, this study found out that the current system quality is on a declining path as evidenced by negatively skewed coefficients. This suggests that the quality of the current system in use is deteriorating. One could infer that the current system at UNW is not meeting the demands of the university community. The finding further shows the mean values are in excess of the median confirming that the quality of electronic systems at the university is being questioned.

The variance and standard deviation forms the integral part of the analysis about the quality of the system because it describes how spread out the data is. If the data all lies close to the mean, then the standard deviation will be small, while if the data is spread out over a large range of values, standard deviation will be large. One of the flaws involved with the standard deviation, is that it depends on the units that are used. One way of handling this difficulty, is called the coefficient of variation which is the standard deviation divided by the mean times 100%

4.2.5 Information Quality

Table 4-6: Information Quality

	Minimum	Maximum	Mean	Std. Deviation	Skewness
Accuracy: The network connected to the Electronic Security System is always in good working order	2	5	3.27	.980	.358
Reliability: The Electronic security services is reliable when coming to getting information more especially getting footages from surveillance cameras	2	5	3.60	1.070	-.188
Relevancy: The Electronic security system provides relevant information	2	5	3.67	.884	.095
Easiness: The Electronic security provides easy-to-understand information.	2	5	3.47	.937	-.032

	Minimum	Maximum	Mean	Std. Deviation	Skewness
Electronic Security System keeps information security risks to a minimum	2	5	3.57	.935	-.071
Information provided by the Electronic Security System meets customer's needs.	2	5	3.57	1.073	-.275

The table 4.6 above addresses the information quality provided by the electronic security system in North West University Mafikeng campus. The respondents rated the accuracy of the network connected to the system as in good working order because the mean value of 3.27 which is more than 3. The scale is between 1 and 5, where 1 represent strongly disagree, 3 represent undecided and 5 represent strongly agree. There is a positive skewness which means that the respondents agree with the accuracy of the network connectivity,

Respondents are asked to rate the Electronic Security System on a series of attributes on a 5-point scale. The mean for a group of thirty respondents for "Accuracy on the information quality" was 3.27 with a Standard Deviation of 0.980 and the mean for "system reliability" was 3.60 with a Standard Deviation of 1.070. At first glance (looking at the means only) it would seem that reliability was rated higher than accuracy.

But the higher Standard Deviation for reliability could indicate (as shown in the distribution above) that responses were very polarized, where most respondents had no reliability issues (rated the attribute a "5"), but a smaller, but important segment of respondents, had a reliability problem and rated the attribute "2". Looking at the mean alone tells only part of the story, yet all too often. The Standard Deviation provides a valuable descriptive measure of this Electronic Security System.

4.2.6 What services will you be interested in on the Electronic Security System

Table 4-7: What services will you be interest in on the Electronic Security

	Minimum	Maximum	Mean	Std. Deviation	Skewness
Good working access control	1	5	2.90	1.155	-.224
Increase customer trust	1	4	2.43	1.073	.095
Reliable system	1	4	2.60	1.133	-.189
Efficient system	1	5	3.00	1.232	-.356
Effective system	1	5	3.07	1.143	-.435
Operational controls	1	4	2.83	.913	-.523
Safety and protection	1	5	2.83	1.262	-.106
Good service delivery	1	5	2.93	1.172	-.275
Impact on business	1	5	2.80	1.095	-.250
System user friendly	1	5	2.70	1.055	-.098
Technological advancement	1	5	2.80	1.126	-.198
Improve customer services	1	4	2.73	1.143	-.474

The main purpose of the Electronic Security System is protecting the university from threats of all kinds, and ensuring the safety and security of the many men and woman that work in these facilities. That's why the university has always looked for ways to improve the security and safety of these facilities and to help in comforting people when they need it most. The university had to find ways to get the experienced and experts to deliver quality security to almost entire university facilities.

NWU required the reliable, efficient, effective, and good working Electronic Security System which is user friendly with good operational controls and which offers good service delivery. According to the table 4.7 above, the respondents with regard to the services offered by the system installed within the campus shows that the services offered are not efficiently and effectively delivered by the system in place because the mean indicate that the response is between 3 and 4, meaning the respondents were not interested in the services provided by the system.

A smaller standard deviation means greater consistency, predictability and quality. The key point is that the standard deviation is an objective measure of variation. Focusing on minimizing the standard deviation of key process characteristics will result in higher quality and customer satisfaction. The standard deviation is above zero which means that most of the respondents were totally against the system.

Most of the data are skewed to the left have a long tail that extends to the left. An alternate way of talking about a data set skewed to the left is to say that it is negatively skewed. In this situation the mean and the median are both lesser than the mode. As a general rule, most of the time for data skewed to the left, the mean will be lesser than the median, which means that most of the respondents were not very interested in the system in the campus.

4.2.7 Service Delivery Output

Table 4-8: Service Delivery Output

Standard of service	Minimum	Maximum	Mean	Std. Deviation	Skewness
Electronic security system provides reliable services.	1	5	3.43	1.006	-.349
Electronic security system responds promptly to information security attacks	2	5	3.70	1.055	-.098
Electronic Security system achieves security compliance with legislation or industry requirements	2	5	3.63	.999	-.061
Electronic Security System is designed with customers' best interest at heart	1	5	3.53	1.137	-.767
Electronic Security System is designed to satisfy the needs of customers	2	5	3.60	.894	-.322
Types of services offered by Electronic Security System are of good quality	1	5	3.33	1.155	-.139
Safety and reliance offered by Electronic Security System are accurate	1	5	3.60	.894	-.632
Standard of service	Minimum	Maximum	Mean	Std. Deviation	Skewness

Electronic Security System helps with prevention of unauthorized access	1	5	3.40	1.221	-.361
---	---	---	------	-------	-------

The service delivery output of the Electronic Security Services is very important and useful for the university because it impacts on the heavily on the running of the business for the entire university. According to Chen, *et al* (2011), strengthening service delivery is a key strategy to achieve the development Goals. This includes the delivery of interventions to reduce crime in the university.

This section focuses on monitoring service delivery output of the electronic Security System in Mafikeng Campus, notably physical access to services. Such data need to be complemented by other dimensions of access and technical quality (safety, efficiency, and effectiveness of selected interventions). According to the respondents in the table 4.5.3 above, shows that the service delivery output is effective, though the quality of the service offered by the Electronic Security Service is still questionable, that is shown by the mean in the table above.

The standard deviation shows that the response with regard to the service delivery output is not up to standard. A low standard deviation indicates that the data points tend to be close to the mean of the set, while a high standard deviation indicates that the data points are spread out over a wider range of values. The data are skewed to the left have a long tail that extends to the left. An alternate way of talking about a data set skewed to the left is to say that it is negatively skewed, which shows that the system is effective.

4.3 LINK TO THE NEXT CHAPTER

The data has been analysed and interpreted in this chapter. In the next chapter, the discussion, recommendation and conclusion of the same data analysis will be made. Ultimately the solutions to the problem will be made available for management to take decisions upon the recommendations and conclusion reached.

CHAPTER FIVE - DISCUSSION, RECOMMENDATIONS AND CONCLUSIONS

5.1 INTRODUCTION

This chapter outlined a brief conclusion from the previous chapters on the effectiveness and efficiency of the Electronic Security System in North West University, Mafikeng Campus. This chapter aimed to bring judgment reached after consideration on the current situation and challenges facing North West University, Mafikeng Campus regarding Electronic Security System so that resolution and decision can be made. Sajkowsky (2006) shows that the analysis indicate that the system has no sustainability in terms of service delivery.

The critical part of this study was to establish whether the university has strategies in place to deal with the identified problems. Sajkowsky (2006) showed that the analysis was conducted to measure the service delivery by the Electronic Security Services and how efficient and effective the services are being offered by the current system.

The results of the analysis will probably only identify and pick up where the problem lies with the Electronic Security System. The responses from the data points from which to extrapolate and interpolate service delivery at the University, describes the percentage of people that receive different levels of system services and it also describes the levels of satisfaction that people have with the service they receive.

Rather than assume that basic service delivery is a straightforward exercise, the university need to analyse the procedures behind service provision. The Protection Services need to ask whether things measured are the best indicators of reliable, relevant and sustainable service for the development of the university.

The Department of Protection Services need to listen more to the recipients of these services and learn from them where the gaps and failures in system design and execution exist. According to Sajkowsky (2006), the Department of Protection Services require lasting and sustainable solutions in order to improve the services offered by the Electronic Security Services.

To effectively address the challenges of the Electronic Security Services, certain processes and procedures need to be adhered and followed. According to Sajkowsky (2006), there is a need for an improvement within the Security department for development, and achievement of efficient, effective and reliable service, and improvement of business processes, systems, decision rights and safety management.

5.2 DISCUSSION

Sabotage usually consists of the destruction of an organization's assets in an attempt to cause loss of confidence on the part of its customers. There are many ways to help protect university from some of these attacks but one of the most functional precautions is user carefulness. According to Belanger, Hiller and Smith (2002), from a business perspective, electronic security system must be in place at all times and functional to fight against crime.

5.2.1. How to analyse the nature of the electronic security system during the student protest?

The electronic security system was not in a good state, which means the system was not fully functional, everyone could get access through the main gate with or without proper, valid access card and the people could exchange the access cards without being noticed and there was a high level of vulnerability and threats in the campus. Most of the assets, students and employees were not protected and safe. The unnecessary and unwanted intrusion would occur without a trace.

The electronic security system components were very much exposed to everyone that is why most of the students could temper with the system during the protests. Cables were cut, CCTV camera were switched off and cut off, and even people who were not part of the university could access the university and disrupts the services of the campus.

5.2.2 How to analyse the effectiveness of the electronic security system at the time of the protest?

The university required the reliable, efficient, effective, and good working Electronic Security System which is user friendly with good operational controls and which offers good service delivery. The respondents with regard to the services offered by the system installed within the campus shows that the services offered are not effectively delivered by the system in place meaning the respondents were not interested in the services provided by the system.

The system was not always in working order and not useful to the customers, therefore the system was not serving any good purpose because the services was intermittent and inconsistent. The system was not reliable and not safe to the users. Therefore, proper and upgraded system should be installed. A fully functional and user-friendly system must be in place at all time, to help identify the intruders when situations are not conducive and favourable

5.2.3 How to analyse the efficiency of the security system in delivering the service?

The efficiency of the security system is measured by how quick or fast is the response towards the attack or intrusion. In the second case is to observe that the service is no longer efficient, the result being negative. According to Beck (2007), this kind of security systems was not chosen randomly, it is by far the most important system (way) of preventing theft in commercial spaces and also in documenting the events, but the system does not deliver what it is meant to do.

Regarding other systems, the alarm systems are very good in preventing and detecting the theft attempts after business hours and it is working intermittently due to lack of continuous maintenance. Above all the service provider reside very far from the campus and comes once in a while for maintenance of the system. Guarding is very efficient in maintaining the order in the commercial spaces, and access control systems have a limited role, mostly to control person access in some areas.

5.2.4. Which electronic security system will give best results for NWU Mafikeng campus?

The system that is very much convenient, user friendly, reliable and safe to use at any time will be best system to rely on in the institution of higher learning like North West University. Electronic security system which respond promptly to information security attacks. Electronic Security system which achieves security compliance with legislation or industry requirements and which meet the needs of the customers. The best quality electronic security system with the best technological advancement.

5.2.5. What impact does the installed system have in a day to day running of the business?

The electronic security system affects the business greatly because the thefts will not be traced effectively and on time. The university will start to run at a loss because of losing assets and pay for lost assets. The dysfunctional system creates lot of unnecessary physical checks, and that creates lot building up of queues at the main entrances and that result in impatience of the customers. Poor service delivery and customer dissatisfaction will start to increase and that will cause a negative impact in the running of the business. The electronic security will provide added value and effectively contribute to the operation of the university only if it is designed and implemented as a core ingredient of the business strategy

5.3 RECOMMENDATIONS

The management should implement security measures in line with their respective security policies in order to mitigate identified risks. According to Stoneburner (2002), the management should have appropriate security solutions in place to protect university assets, students, employees and communication links against abuse or attacks. All changes should be subject to a formal change management process ensuring that changes are properly planned, tested, documented and authorized.

On the basis of the changes made and the security threats observed, tests should be repeated regularly and include scenarios of relevant and known potential attacks. Trusted and independent (internal or external) experts should carry out the audits. They should not be involved in any way in the development, implementation or operational management of the Electronic Security Services provided.

From a technical point of view, a secure closed system (i.e., one acceptably resistant to external attack, accidental disclosures, internal subversion, and denial of use to legitimate users) while presenting difficult problems, can be provided by contemporary technology; but a secure open system cannot be provided by contemporary technology. In fact, there is special concern about the risk of compromise of classified information and the vulnerability of an open system to potential penetrations

5.4 CONCLUSION

The responsiveness of the security system to threats is very much important to eliminate the vulnerabilities and threats beforehand and to avoid unnecessary costs against the university. The risk assessment should be conducted to

Responses to threats

- reduce/mitigate – implement safeguards and countermeasures to eliminate vulnerabilities or block threats
- assign/transfer – place the cost of the threat onto another entity or organization such as purchasing insurance or outsourcing
- Accept – evaluate if cost of countermeasure outweighs the possible cost of loss due to threat, do nothing.
-

The risk assessment report:

- Summarizes the system architecture and components, and its overall level of security;
- Includes a list of threats and vulnerabilities, the system's current security controls, and its risk levels;
- Recommends safeguards, and describes the expected level of risk that would remain if these safeguards were put in place;

- Shows where an organization needs to concentrate its remedial work;
- Can be used as input to the university's business continuity plan; □ Presents these findings to management.

The university should do everything in its power to provide an increased and improved service over time. Effective and efficient service delivery will bring about good and successful results, and that will make customers happy at the end of the day. The question should be asked as to how sustainable the current levels of service delivery are and whether they are likely to show an improvement or a decline.

The management should follow processes and procedures of the security act in order to ensure that the entire university is safe and secure and to address security assurance in a comprehensive manner in the university in order to deal with unnecessary crime and the vulnerabilities taking place in the campus. According to Takabi, Joshi, and Ahn (2010) July. (pp. 393-398), management has to deal with the following multiple tasks to make sure that everything is in order:

- Acquiring or develop a well-tested security-enhanced process or methodology that best fits development culture of the organization.
- Making the fundamental changes to the organizational process that help in smoothly implementing the security cross checks and measuring the benefits in terms of metrics.
- Creating security awareness at each and every level in the organization. This may require running different training programs, tailored to meet the interests of their respective target audience.
- Equipping the consultants on job with the right kind of tools and guidance and providing adequate and support.
- Implementing processes to audit the security posture and manage the vulnerability life cycle.
- Implementing processes to track the latest happening in the campus, in terms of best practices, recent trends in the vulnerability attacks, new vulnerability remediation techniques and so on and to update the university's own process/ checklists/ guidelines accordingly.

5.5 AREAS FOR FUTURE RESEARCH

The following research topics have been identified for future research, namely:

- Policy, model and design of the security architecture.
- Securing data transfer in wired and wireless communications, especially security issues on low power devices.
- Examining the security of the interfaces between different components (e.g., operating system, database system, and logging mechanism) and ensuring that no security loopholes are introduced due to component interactions.
- Integrating Security and enhancing sustainability

The research should also look at providing for sustainable design that meets all facility requirements which is often a challenge.

REFERENCE

Belanger, F., Hiller, J.S. & Smith, W.J. 2002. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The journal of strategic Information Systems*, 11(3): 245-270.

Bhattacharjee, S., Roy, P., Ghosh, S., Misra, S. & Obaidat, M.S. 2012. Wireless sensor network-based fire detection, alarming, monitoring and prevention system for Bord-andPillar coal mines. *Journal of Systems and Software*, 85(3): 571-581.

Boellaard, R., 2009. Standards for PET image acquisition and quantitative data analysis. *Journal of Nuclear Medicine*, 50 (1): 11S-20S.

Bosch JJ, Rathi P, Howcroft KM, West RM, inventors; JP Morgan Chase Bank, assignee. Account opening system, method and computer program product. United States patent US 8,224,723. 2012 Jul 17.

Bosch Security Systems. 2009. Access control by example: introductory guide. Ottobrunn: Bosch Security Services
http://resource.boschsecurity.com/documents/application_note_enus_1211005195.pdf
Date of access: 27 Nov. 2017.

Bowers, L., Crowhurst, N., Alexander, J., Callaghan, P., Eales, S., Guy, S., McCann, E. and Ryan, C., 2002. Safety and security policies on psychiatric acute admission wards: results from a London-wide survey. *Journal of Psychiatric and Mental Health Nursing*, 9(4), pp.427-433.

Broder, J.F. & Tucker, E. 2011. Risk analysis and the security survey. Wlatham: Butterworth-Heinemann.

Bye, S.J., Paczkowski, L.W., Parsel, W.M., Persson, C.J., Schlesener, M.C. and Shipley, T.D., Sprint Communications Co LP, 2015. *Systems and methods for provisioning and using multiple trusted security zones on an electronic device*. U.S. Patent 9,183,412.

Chen, C.C., Liu, J.Y.C. & Chen, H.G. 2011. Discriminative effect of user influence and user responsibility on information system development processes and project management. *Information and Software Technology*, 53(2): 149-158.

Collins, P.A., Ricks, T.A. & Van Meter, C.W., 2015. Principles of security and crime prevention. London: Routledge.

Compartmented, S., 2013. Unified Facilities Criteria (UFC). *Change*, 1:1 - 2.

Creswell, J.W., 2013. Research design: Qualitative, quantitative, and mixed methods approaches. Thousand Oaks: Sage publications.

Crowe, T.D. & Fennelly, L.J., 2013. Crime prevention through environmental design. Waltham, MA: Butterworth-Heinemann.

DiMase, D., Collier, Z.A., Heffner, K. & Linkov, I., 2015. Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions*, 35(2): 291-300.

Enders, C. K. 2010. Applied missing data analysis. London: Guildford Press.

Fatima, A., 2015. E-Banking Security Issues? Is There A Solution in Biometrics? *The Journal of Internet Banking and Commerce*, 16 (2): 1 – 9

Foodman, B.A. & Foodman, H.W., Radia Technologies Corporation, 2005. Internet based security, fire and emergency identification and communication system. U.S. Patent 6,975,220.

Gerstner, W., 2006. Population dynamics of spiking neurons: fast transients, asynchronous states, and locking. *Population*, 12(1).

Haggerty, K.D., 2004. Ethics creep: Governing social science research in the name of ethics. *Qualitative sociology*, 27(4): 391-414.

Haren, E.D. & Lai, A.J. 2007. Electronic device security system and method. U.S. Patent Application 11/799,186.

Hwang, M.S. & Li, L.H., 2000. A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 46(1): 28-30.

Hyatt Jr, R.G., Trent, D. & Hall, C.1998. Electronic security system. U.S. Patent 5,745,044.

Johnson, B. & Turner, L.A., 2003. Data collection strategies in mixed methods research. *Handbook of mixed methods in social and behavioral research*, pp.297-319.

Krause, P.R., 2006. Method and apparatus for enhancing electronic reading by identifying relationships between sections of electronic text. U.S. Patent 7,143,348.

Lewis, S., 2015. Qualitative inquiry and research design: Choosing among five approaches. *Health promotion practice*, 16(4): 473-475.

Marianetti, R. & Hawkins, J.C. 2003. Mobile computer system capable for copying set-up application including removal routine from peripheral device for removing device programs after the device is removed. U.S. Patent 6,539,476.

Nazareth, D.L. and Choi, J., 2015. A system dynamics model for information security management. *Information & Management*, 52(1): 123-134.

Norman, T.L., 2011. Electronic access control. London: CRC Press

Norman, T.L., 2016. Risk analysis and security countermeasure selection. London: CRC press.

Olckers, C. 2007. An examination of the impact of residential security measures on the incidence of residential burglary in two selected northern suburbs of Johannesburg: A security risk management approach. Unpublished MTech dissertation. Pretoria: University of South Africa.

Paris, C.B., Helgers, J., Van Seville, E. and Srinivasan, A., 2013. Connectivity Modeling System: A probabilistic modeling tool for the multi-scale tracking of biotic and abiotic variability in the ocean. *Environmental Modelling & Software*, 42, pp.47-54.

Pieprzyk, J., Hardjono, T. & Seberry, J., 2013. Fundamentals of computer security. New York: Springer Science & Business Media

Redlich, R. M. & Nemzow, M. A. 2000. Data security system and method responsive to electronic attacks. Florida: Digital Doors, Inc. URL Date of access: 17 May 2018.

Ryder, S., Apple Inc., 2016. One step security system in a network storage system. U.S. Patent 9,319,408.

Sajkowsky, J.M., United Security Applications Id, Inc., 2006. Electronic security system for monitoring and recording activity and data relating to cargo. U.S. Patent 7,012,529.

Saparkhojayev, N. & Guvercin, S., 2012. Attendance Control System based on RFID technology. *IJCSI International Journal of Computer Science Issues*, 9(3), pp.1694-0814.

Semertzidis, T., Dimitropoulos, K., Koutsia, A. & Grammalidis, N., 2010. Video sensor network for real-time traffic monitoring and surveillance. *IET intelligent transport systems*, 4(2): 103 - 112.

Sennewald, C.A. & Baillie, C., 2015. Effective security management. Burlington: Butterworth-Heinemann.

- Shen, C., Everitt, K. & Ryall, K., 2003. UbiTable: Impromptu face-to-face collaboration on horizontal interactive surfaces. In *UbiComp 2003: Ubiquitous Computing* (pp. 281-288). Springer Berlin/Heidelberg.
- Shirlen, M.R. & Hofmann, R.G., Qualcomm Incorporated, 2014. Method for securely communicating information about the location of a compromised computing device. U.S. Patent 8,839,460.
- Simmons, J.P., Nelson, L.D. and Simonsohn, U., 2011. False-positive psychology: Undisclosed flexibility in data collection and analysis allows presenting anything as significant. *Psychological science*, 22(11), pp.1359-1366.
- Stoneburner, G., Goguen, A.Y. and Feringa, A., 2002. Risk management guide for information technology systems. <https://csrc.nist.gov/publications/detail/sp/80030/archive/2002-07-01> Date of access 27 Nov. 2017.
- Subashini, S. and Kavitha, V., 2011. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, 34(1): -11.
- Surette, R., 2005. The thinking eye: Pros and cons of second generation CCTV surveillance systems. *Policing: An International Journal of Police Strategies & Management*, 28(1): 152-173.
- Takabi, H., Joshi, J.B. and Ahn, G.J., 2010, July. Securecloud: Towards a comprehensive security framework for cloud computing environments. In *Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual* (pp. 393398). IEEE.
- United States Corps of Engineers, 2013, electronic Security System (ESS) is the integrated electronic system that encompasses the Access Control System (ACS).
- Veres, A., Gray, Michel, J.B., Shen, Y.K., Aiden, A.P M.K., Pickett, J.P., Hoiberg, D., Clancy, D., Norvig, P., Orwant, J. and Pinker, S., 2011. Quantitative analysis of culture using millions of digitized books. *Science*, 331(6014), pp.176-182.
- Zittrain, J., 2008. The future of the internet--and how to stop it. Yale: Yale University Press.

APPENDIXES

APPENDIX A– ETHNICAL CLEARANCES



NORTH-WEST UNIVERSITY
YUNIBESITHI YA BOKONE-BOPHIRIMA
NOORDWES-UNIVERSITEIT

Private Bag X6001, Potchefstroom,
South Africa, 2520

Tel: (018) 299-4900

Faks: (018) 299-4910

Web: <http://www.nwu.ac.za>

Institutional Research Ethics Regulatory Committee

Tel: +27 18 299 4849

Email: Ethics@nwu.ac.za

ETHICS APPROVAL CERTIFICATE OF PROJECT

Based on approval by the **Human Resource Research Ethics Committee (HRREC)** on **04/08/2017**, the North-West University Institutional Research Ethics Regulatory Committee (NWU-IRERC) hereby **approves** your project as indicated below. This implies that the NWU-IRERC grants its permission that, provided the special conditions specified below are met and pending any other authorisation that may be necessary, the project may be initiated, using the ethics number below.

Project title: The effectiveness and efficiency of electronic security system in North West University Mafikeng Campus																												
Project Leader/Supervisor: Dr S Kopung																												
Student: DP Tabane																												
Ethics number:	<table border="1"><tr><td>N</td><td>W</td><td>U</td><td>-</td><td>0</td><td>0</td><td>6</td><td>4</td><td>3</td><td>-</td><td>1</td><td>7</td><td>-</td><td>A</td><td>9</td></tr><tr><td colspan="3">Institution</td><td colspan="3">Project Number</td><td colspan="3">Year</td><td colspan="3">Status</td></tr></table> Status: S = Submission, R = Re-Submission, P = Provisional Authorisation, A = Authorisation	N	W	U	-	0	0	6	4	3	-	1	7	-	A	9	Institution			Project Number			Year			Status		
N	W	U	-	0	0	6	4	3	-	1	7	-	A	9														
Institution			Project Number			Year			Status																			
Application Type: Single Study																												
Commencement date: 2017-08-04	Expiry date: 2020-08-04																											
Risk:	NA																											

Special conditions of the approval (if applicable):

- Translation of the informed consent document to the languages applicable to the study participants should be submitted to the HRREC (if applicable).
- Any research at governmental or private institutions, permission must still be obtained from relevant authorities and provided to the HRREC. Ethics approval is required BEFORE approval can be obtained from these authorities.

General conditions:

While this ethics approval is subject to all declarations, undertakings and agreements incorporated and signed in the application form, please note the following:

- The project leader (principle investigator) must report in the prescribed format to the NWU-IRERC via HRREC:
 - annually (or as otherwise requested) on the progress of the project, and upon completion of the project
 - without any delay in case of any adverse event (or any matter that interrupts sound ethical principles) during the course of the project.
 - Annually a number of projects may be randomly selected for an external audit.
- The approval applies strictly to the protocol as stipulated in the application form. Would any changes to the protocol be deemed necessary during the course of the project, the project leader must apply for approval of these changes at the HRREC. Would there be deviation from the project protocol without the necessary approval of such changes, the ethics approval is immediately and automatically forfeited.
- The date of approval indicates the first date that the project may be started. Would the project have to continue after the expiry date, a new application must be made to the NWU-IRERC via HRREC and new approval received before or on the expiry date.
- In the interest of ethical responsibility the NWU-IRERC and HRREC retains the right to:
 - request access to any information or data at any time during the course or after completion of the project;
 - to ask further questions, seek additional information, require further modification or monitor the conduct of your research or the informed consent process.
 - withdraw or postpone approval if:
 - any unethical principles or practices of the project are revealed or suspected,
 - it becomes apparent that any relevant information was withheld from the HRREC or that information has been false or misrepresented,
 - the required annual report and reporting of adverse events was not done timely and accurately,
 - new institutional rules, national legislation or international conventions deem it necessary.
- HRREC can be contacted for further information via Estie.Emtch@nwu.ac.za or 018 289 2873.

The IRERC would like to remain at your service as scientist and researcher, and wishes you well with your project. Please do not hesitate to contact the IRERC or HRREC for any further enquiries or requests for assistance.

Yours sincerely

Prof LA

Du Plessis

Digitally signed by

Prof LA Du Plessis

Date: 2017.09.01

13:02:42 +02'00'

Prof Linda du Plessis

Chair NWU Institutional Research Ethics Regulatory Committee (IRERC)

APPENDIX B – LETTER OF EDITING



NORTH-WEST UNIVERSITY
YUNIBESITHI YA BOKONE-BOPHIRIMA
NOORDWES-UNIVERSITEIT
MAFIKENG CAMPUS

Department of Academic Literacy

05 July 2018

Private Bag X2046

Mmabatho

2735

CERTIFICATE OF EDITING A DISSERTATION

TO WHOM IT MAY CONCERN

This serves to confirm that I have read and edited Mr. D. P. Tabane's dissertation titled: **The effectiveness and efficiency of electronic security system at the North-West University, Mafikeng Campus**. The candidate corrected the language errors identified. The document is of an acceptable linguistic standard.

Thank you

Yours Faithfully

A handwritten signature in grey ink, appearing to read 'J.R. Moletsane'.

.....
J.R. Moletsane (Subject Head Academic Literacy)

Accr. No. 1002708

joel.moletsane@nwu.ac.za