AN EXAMINATION OF THE EFFECTIVENESS OF PHYSICAL SECURITY MEASURES AT GOVERNMENT PRINTING WORKS, PRETORIA

By

DUMISI DANIEL MOKOENA

STUDENT NUMBER: 47534001

Submitted in accordance with the requirements for the degree of

MAGISTER TECHNOLOGIAE

In the subject

SECURITY MANAGEMENT

at the

UNIVERSITY OF SOUTH AFRICA

Supervisor

PROF K. PILLAY

30 April 2023

DECLARATION

Name: Dumisi Daniel Mokoena

Student number: 47534001

Degree: Master Artium in Criminal Justice (Security Management)

AN EXAMINATION OF THE EFFECTIVENESS OF PHYSICAL SECURITY MEASURES AT GOVERNMENT PRINTING WORKS, PRETORIA

I declare that the above dissertation is my work and that all the sources I have used or quoted have been indicated and acknowledged employing complete references.

I further declare that I submitted the dissertation to originality-checking software, which falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

30 August 2023

SIGNATURE: **DATE:**
MR DD MOKOENA

COPYRIGHT

Unisa 2023

ACKNOWLEDGEMENTS

First, I praise God, Father in heaven, who gave me the courage, knowledge, and endurance to complete this research.

I am very much grateful to my elegant wife, Mrs. Mamphaki Kedibone Mokoena, and my three beautiful children, Lebohang Lovedelia Mokoena, Dineo Daphney Mokoena and Lethabo Lesley Mokoena, who always believed and stood by me through hectic years of my studies. Your sacrifice has taught me that having a dream is one thing, and working towards achieving it and finally achieving it is another. I will always cherish this achievement dedicated to all of you.

Furthermore, I would also like to express my sincere gratitude to the following persons for their respective contributions:

- My late parents, Nyalasi Solomon Mokoena and Sesi Rebecca Mokoena; my late siblings (Mkhanyela Samuel Mokoena, Sebolelo Esther Mokoena, and Ditaba John Mokoena) who always provided me with endless support and motivation throughout my life and instilled qualities in me that enabled me to complete this study. May their soul continue to rest in eternal peace.

- My adorable sisters (Maki Alinah Mokoena, Nkokoto Elizabeth Mokoena, Matebello Maria Mnguni, Maphakisa Emily Mokoena, and Makhala Anah Mokoena), for your unwavering support through the difficult times of my life. Thank you for never giving up on me when I could not afford the time to spend with you. Now is the time to wind down!

- My research supervisor, Professor Kris Pillay (Ph.D.), for his valuable advice, encouragement, and inspiration during the tough times of this study and for directing me to the winning path when everything seemed to be crumbling; thank you!

- Finally, a special thanks to the Government Printing Works (GPW): CEO (Ms. Alinah Fosi) for permitting me to conduct my research within GPW.

- Importantly, special thanks go to all interview participants for their willingness to be open throughout the data collection process.

EXECUTIVE SUMMARY

Government Printing Works (GPW) has a long history of creating and publishing national documents such as birth certificates, passports, and identification documents. If these records are compromised in any manner, South Africa could face grave security challenges. Similarly, unauthorised access to these documents can have devastating effects on national security. The purpose of this study was to examine the efficiency of physical security measures at Government Printing Works. The research employed a qualitative methodology. The exploratory research design was selected. The technique of convenience sampling was employed to select 20 participants. As a research tool, semi-structured interviews using an interview guide were employed. The findings of the study indicate that employees anticipate enhanced physical security measures to ensure the physical safety of Information Technology (IT) assets, such as facilities, equipment, personnel, and property protection. The current security at GPW was found to be good albeit some weaknesses. The results shows it's hard to come with a water tight physical security. In addition, it was discovered that strong leadership is a strength of the physical security measures at GPW, while a lack of communication is main weakness. The current study suggests that GPW augment its physical security by installing signs, fences, and other barriers, sufficient lights, patrols, alarms for obstacles, additional indoor and outdoor CCTV cameras, doors, locks, security personnel, and access control systems.

Keywords; Access control; effectiveness; Closed-Circuit Television; physical security; qualitative; risk; security breach; security measures; strengths; thematic; weaknesses.

KGUTSUFATSO YA PHETHAHATSO

Ofisi ya Dikgatiso tsa Mmuso (GPW / Government Printing Works) e na le nalane e telele ya ho hlahisa le ho phatlalatsa ditokomane tsa naha tse kang mangolo a tswalo, diphasepoto, le ditokomane tsa boitsebiso. Haeba direkoto tsena di ka behwa tsietsing ka mokgwa leha e le ofe, Afrika Borwa e ka tobana le diphepetso tse matla tsa tshireletso. Ka ho tshwana, phumantsho e sa dumellwang ya ditokomane tsena e ka ba le ditlamorao tse mpe mabapi le tshireletso ya naha. Morero wa diphuputso tsena e ne e le ho hlahloba bokgabane ba mehato e tshwarehang ya tshireletso dikantorong tsa Mesebetsi ya Dikgatiso tsa Mmuso. Diphuputso di sebedisitse mokgwa wa diphuputso wa dipalo *(qualitative methodology).* Ho ile ha kgethwa moralo wa diphuputso wa ho fatolla *(exploratory research)*. Lewa la ho sebedisa disampole tse haufinyana tse leshome le metso emebedi le ile la sebediswa. Jwalo ka sesebediswa sa diphuputso, dipuisano tse hlophisitsweng habonolo di ile tsa sebediswa. Diphetho di bontshitse hore basebeletsi ba lebeletse mehato e matlafaditsweng ya tshireletso ho netefatsa polokeho e bonahalang ya dithoto tsa mahlale a dikomporo (Information Technolgy), tse kang dibaka, thepa, basebeletsi, le tshireletso ya moaho. Tshireletseho ya ha jwale ho GPW e fumanwe e le ntle le ha e le mefokolo e meng. diphetho di bontsha hore ho thata ho tla le tshireletso e tiileng. Hodima moo, ho ile ha sibollwa hore maitsebelo a matla a boetapele ke tshiya ya ditsela tse tshwarehang tsa tshireletso ofising ya Dikgatiso tsa Mmuso, ha kgaello ya ho buisana e le bofokodi bo teng. Diphuputso tsa hajwale di sisinya hore ofisi ena ya Dikgatiso tsa Mmuso e eketse tshireletso ya yona e tshwarehang ka ho kenya matshwao, difense le dithibelo tse ding, mabone a lekaneng, dipatrolo, dialamo bakeng sa ditshitiso, dikhamera tsa CCTV ka ntle le ka hare, mamati, dinotlolo, balebedi le mekgwa ya ho laola ho kena le ho tswa.

Mantswe a Sehlooho; Ho tswa le ho kena; Kgaello ya tshireletso, kotsi, dikhamera tsa CCTV, mehato ya tshireletso, tshireletso e tshwarehang, matla, bofokodi, , tsa boleng, tsa mookotaba, bokgabane.

BEKNOPTE OORSIG

Die Staatsdrukkery (GPW / Government Printing Works) het ’n lang geskiedenis wat gekenmerk word deur die skepping en publisering van nasionale dokumente soos geboortesertifikate, paspoorte en identiteitsdokumente. Indien hierdie rekords op enige wyse gekompromitteer sou word, kan Suid-Afrika ernstige sekuriteitsuitdagings in die gesig staar. Net so kan ongemagtigde toegang tot hierdie dokumente rampspoedige gevolge vir nasionale sekuriteit hê. Die doel van hierdie studie was om die doeltreffendheid van fisieke beveiligingsmaatreëls by die Staatsdrukkery te ondersoek. ’n Kwalitatiewe metodologie is in die navorsing gebruik. Die verkenningsnavorsing-ontwerp en die tegniek van gerieflikheidsteekproefneming is ingespan. As navorsingshulpmiddel is halfgestruktureerde onderhoude met die hulp van ’n onderhoudsgids, gebruik. Die resultate van die studie dui daarop dat werknemers versterkte maatreëls vir fisieke beveiliging verwag om die fisieke veiligheid van IT-bates, soos fasiliteite, toerusting, personeel, en eiendomsbeskerming te verseker. Daar is ook ontdek dat sterk leierskapsvaardighede ’n sterk punt van die fisieke beveiligingsmaatreëls by die Staatsdrukkery is, terwyl ’n gebrek aan kommunikasie ’n swakheid is. Die huidige studie stel voor dat die Staatsdrukkery sy fisieke sekuriteit aanvul deur uithangtekens, heinings en ander versperrings, genoegsame beligting, patrollies, alarms vir hindernisse, bykomende binnenshuise en buitenshuise geslotekringtelevisie-kameras, deure, slotte, sekuriteitspersoneel, en toegangsbeheerstelsels in te span.

Sleutelwoorde: Toegangsbeheer; doeltreffendheid; geslotekringtelevisie; fisieke beveiliging; kwalitatief; risiko; Sekuriteitsoortreding; beveiligingsmaatreëls; sterk punte; tematies; swakhede.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

GPW	Government Printing Works
AACS	Automated Access Control Systems
CCTV	Closed-Circuit Television
CSSS	Copenhagen School of Security Studies
IoT	Internet of Things
IT	Information Technology
NKP	National Key Points
PSIRA	Private Security Industry Regulatory Authority
SABC	South African Broadcasting Corporation
SPF	Security Printing Facility
X-ray	X-Ray machine

CHAPTER 1: INTRODUCTION AND MOTIVATION FOR RESEARCH

1.1 Introduction

The Government Printing Works (GPW) located in the city of Tshwane came into existence when the former House of Assembly gave the South African government permission to set up a proper government printing press in 1888 (Milubi, 2020). The GPW has a long history of producing and printing critical national documents, including birth certificates, passports, and identification documents. The GPW is primarily responsible for printing documents for government departments, with some containing sensitive information (Milubi, 2020). If these documents are compromised in any way, it may lead to serious security threats for South Africa. Therefore, examining the efficiency of physical security measures at the Government Printing Works Security Printing Facility (SPF) is necessary.

Similarly, unauthorised access to these documents can severely damage national security. Security breaches, such as unauthorised access to secure government buildings, may occur anytime. Thus, these buildings require sound physical security systems (Moyo, 2014). This chapter presents the study's background, the research problem, and why the research was done. It also gives an overview of the GPW. The chapter also presents the research questions and objectives and outlines the dissertation.

1.2 Background to the Study

The loss of physical assets is likely due to a lack of well-designed physical security measures (Ai-Phin, Abbas & Kamaruddin, 2020). Poorly designed physical security designs lead to financial and non-financial losses, such as inconveniences caused when key documents are stolen (Ai-Phin et al., 2020). The GPW is considered one of Africa's most forward-thinking security printing agencies. It has a high-tech production, printing, and distribution plant that is one of the most modern in the world (Clarke & Kuipers, 2015). Therefore, implementing effective physical security control measures is essential in reducing security risks, especially in an organisation such as the GPW, whose mandate is critical to all South Africans. The GPW offers various services, including printing identification documents, passports, birth certificates, and national senior certificate examination papers. Nonetheless, it has been widely speculated that the physical security mechanisms at GPW have flaws (Government Printing Works, 2021).

Shohaieb, Hashem & Hanafy (2018) argue that physical security measures are only effective when applied correctly. Physical security measures include protecting the building and property against natural disasters, fire, burglary, floods, vandalism, terrorism, and theft (Ghazi, 2016; Mohamed, Abas, Hassan & Ismail, 2021; Urhiewhu, Emojorho & Omah, 2018). Therefore, physical security measures play an essential role in protecting property. It prevents the property from experiencing security breaches that may compromise the organisation's security. Security breaches at GPW expose government departments and ministries to security risks. Therefore, examining whether physical security measures are efficient or effective is essential. If they are inefficient or ineffective, then steps should be taken to design mechanisms to protect the organisation and prevent risks.

The study was motivated by the need to understand why there have been breaches of existing security measures resulting in severe financial, reputational, and property losses to the organisation. The GPW premises are regarded as critical infrastructure, and the security measures in and around its operations must be maintained at a maximum level (Office of the Presidency, 2019). Therefore, this study examined the efficiency and effectiveness of physical security measures at the GPW, Pretoria.

1.3 Rationale for the Study

Physical security safeguards assets (Perdikaris 2014). Physical security at GPW has been questioned. GPW's CCTV sometimes malfunctioned, producing black-and-white photos that did not identify the burglar. Also, due to improper alarm pairing, GPW's CCTV system has failed to prevent security breaches (Government Printing Works 2021). The SABC (2020) reports that the Department of Basic Education considers GPW exam paper leaks a major issue. GPW leaked a Grade 12 Physical Science paper in 2020. Exam leakages suggest GPW's physical security has failed to prevent security breaches. The Department of Basic Education engaged GPW to process and print exam papers. Therefore, investigators tracked the leaks to them (SABC, 2020). In addition to exam leakages, thieves broke into the GPW and stole laptops and confidential documents. Air-conditioning systems have been stolen before, affecting

GPW Security Printing Facility machines. Visas and other security-featured certificates were stolen (SABC 2020). These challenges, among others, have threatened the physical security of GPW as a strategic organisation in South Africa.

The findings from this study would fill a knowledge gap in physical security strategies for advanced GPW capacity for suitable physical security at the organisation. During his tenure, the researcher noted a rise in security breaches at the GPW because of the poor implementation of adequate security measures. The researcher observed such poor security measures because of his previous engagement as an employee of the GPW. As such, the researcher became interested in the state of the physical security measures at the GPW in Tshwane. The researcher took a keen interest in the topic after reading and analysing information about how security is implemented for government infrastructure. Because of a lack of information and knowledge on the subject, it was essential to do qualitative research on how well the physical infrastructure works. In addition, the researcher felt this study is critical because it would help GPW employees and other people in the security industry improve their work to deal with the security flaws that have been identified. The study is the first to examine whether the physical security measures at the GPW in Tshwane are effective.

1.4 Problem Statement

The research problem addresses a gap in research that the researcher intends to address (Ochara, 2019). The researcher was motivated to conduct this study at the GPW due to the rising number of security breaches at the organisation (SABC, 2020). The researcher, who was previously employed at the GPW, observed the current physical security measures implemented at GPW and noticed problems with closed-circuit television (CCTV), surveillance cameras, facial recognition mechanisms, security guards, alarm systems, walkthrough detectors, scanners, and automatic security gates.

In some instances, at GPW, the CCTV was hacked and produced black-and-white images which did not identify the intruder. The CCTV system has not effectively stopped security breaches at GPW, as it has sometimes not been appropriately paired with an alarm system. At GPW, the surveillance cameras were intended to dissuade burglars, but they had little influence on people intent on committing a crime because facial recognition was futile on masked thieves. The automatic security gates at GPW rely heavily on electrical power, which is a major problem during load shedding. This means the gates had no power when load shedding occurred. In some instances, the automatic gate was left open for a while due to the lack of a backup generator, increasing the risk of intruders getting inside, knowing there was load shedding. Walkthrough detectors and scanners have been ineffective in detecting weapons criminals possess as they sometimes connive with security officers on duty to get inside. The prior security breaches have cost government departments millions of Rands and caused a lack of public trust in government entities, especially the Department of Basic Education (DBE), which has borne the brunt of exam leakages at the GPW.

According to the SABC (2020), the DBE has identified exam paper leakages at GPW as a severe problem. In 2020, two Grade 12 Physical Science papers were leaked from GPW. This indicates that security measures at the GPW do not prevent security risks from occurring. In the above example, investigators traced the leakages and blamed the GPW as the company hired by the DBE to process and print exam papers (SABC, 2020). Besides the exam leakages mentioned above, intruders bypassed security measures by entering the premises and stealing computers containing confidential information at the GPW. There have been other incidents where air-conditioning systems were stolen, affecting the machines which need them in the SPF. At some point, intruders attempted to steal staff vehicles. There was also the theft of face-value documents, such as visas and other certificates that included security features (Government Printing Works 2021).

These challenges, among others, have threatened the physical security of GPW as a strategic organisation in South Africa. These challenges must be compared to physical security in other nations, such as the UK and Nigeria, where physical security measures have been emulated because they are enhanced to prevent security breaches. The reason could be that there are resources and formulated policies that guide such physical security practices. Could South Africa and GPW encounter physical security because necessary resources may not have been available to capacitate the strategic organisation? The concerns mentioned earlier have necessitated this study on creating a more robust physical security measure. The findings from this study would fill a knowledge gap in physical security strategies for advanced GPW capacity for suitable physical security at the organisation.

1.5 Key Theoretical Concepts

1.5.1 Access Control

Access control is a security feature that controls how people access or enter facilities and other places where access is authorised (Landoll, 2011; Aladejebi & Oladimeji, 2020). Before a person or visitor enters the premises, they must identify themselves and provide valid reasons for visiting. At GPW, access control is implemented since visitors must first state the purpose of their visit to the premises to the security officer on duty, and this will be recorded in the appropriate security register book. There is controlled access to the GPW premises through an inventory of who is on the premises at any given time.

1.5.2 Critical Infrastructure Protection Act 8 of 2019

The Critical Infrastructure Protection Act 8 of 2019 provides rules and considerations to facilitate the transparent identification and declaration of crucial infrastructure (Office of the Presidency 2019). This Act aids the GPW in gaining the confidence of its stakeholders and the entire country (Lewis, 2019).

1.5.3 Government Printing Works (GPW)

The GPW is the state’s authorised printing entity for the South African government (GPW, 2021). It is based in Tshwane, Gauteng, and boasts a high-tech production plant with state-of-the-art equipment (SABC, 2020).

1.5.4 Procedural Control

Procedure control is a set of steps that spell out the steps to be taken and the time and order in which they should be done (Mavroeidis et al., 2018). At the GPW, the search procedure is an example of this kind of procedure. It tells security personnel how to search people legally, politely, and respectfully (Arogundade, Abioye, & Sanjay, 2020).

1.5.5 Physical Security

Physical security involves keeping assets out of the reach of others not authorised to access them (Milubi, 2020). Physical security is defined as access control measures in the facilities, which include buildings, rooms, and information technology peripherals (Ai-Phin et al., 2020; Lukas, 2016). Guards and security escorts support the physical security measures that may exist at the GPW (Milubi, 2020).

1.5.6 Physical Security Controls

Physical security controls are the methods of physical security that protect assets through site design and layout, environmental components, emergency response readiness, training, access control, intrusion detection, and power and fire protection (Harris, 2013). It involves using physical and procedural controls designed to effectively protect organisations, deter intruders, and respond to and recover from intentional and unintentional events that could cause severe loss of critical assets for organisations (Mavroeidis, Vishi & Josang, 2018). Doss, Knopp, Roddy, Rothman, Hatch, & Rhoades (2020) defines physical security controls as any measures to deter and prevent unauthorised access that is put in place to mitigate security-related issues. Some physical control measures at the GPW include CCTV cameras which monitor or provide surveillance of the building, motion detection alarm systems, and security guards operating the facilities.

1.5.7 Physical Security Programmes and Measures

These measures or programs prevent unauthorised access to equipment, installations, materials, and documents (Perdikaris, 2014). The physical security program at the GPW includes CCTV cameras, biometric access control, and security guards. Often known as video surveillance, CCTV uses video cameras to relay a signal to a specified location on a restricted number of display screens (Doss, Knopp, Roddy, Rothman, Hatch & Rhoades, 2020). According to Raj, Gadde & Jayaraman (2021), a biometric access control system is a technology that decides whether or not a person may enter a building or a particular room based on the individual’s unique biometric characteristics. It compares a unique individual characteristic, such as the face, fingerprint, iris, palm, and hand geometry, to a database containing biometric templates of authorised users. If there is a match, the individual is granted admission;

otherwise, they are refused entry. It offers substantial physical security advantages for defending various venues from invaders (Raj et al., 2021). At the GPW, CCTV cameras monitor or provide surveillance of the building, and security guards are employed in-house to operate the facilities. However, a biometric system is yet to be implemented.

1.5.8 Security

Security is defined as the feeling of being safe and secure, which includes the lack of threats and the management of future risks (Jore, 2019). The term security is derived from the Latin noun "securitas," which means freedom of fear, safety, and a guarantee of conditions and circumstances (Nemeth, 2018). Security, therefore, means being protected from harm or risks. Private security officers are responsible for this at the GPW (Milubi, 2020).

1.5.9 Security Breach

According to Milubi (2020), security breach occurs when an unauthorised individual accesses a system. Once intruders access the system on the premises, they do illegal things; for instance, at the GPW, people leak exam papers and have blueprints of identification documents to make counterfeit identity documents (IDs). This corresponds to a security breach at the GPW in that those involved reproduce fake IDs.

1.5.10 Security Risk Management

Security risk management includes figuring out how likely and dangerous possible attacks are and taking steps to make them less likely and less risky (Jore, 2019; Milubi, 2020). At the GPW, the security team is responsible for identifying the different security risks and the best way to deal with them.1.6 Research Aim and Objectives

1.6.1 Aim of the Study

The research aim should express the study's intention and precisely summarise in a single sentence what the researcher intends to achieve at the end of a research project (Bailey, Doody & Lyons, 2016). The aim of the study is to examine the effectiveness of physical security measures at the GPW in the City of Tshwane.

1.6.2 Research Objectives

Research objectives are the desired outcomes the researcher sets when conducting research. Research projects usually have multiple objectives (Bailey et al., 2016). The following are the objectives of the study:

- To evaluate the current state of physical security measures at GPW.
- To determine the strengths and weaknesses of the current physical security measures at GPW.
- To make recommendations to the GPW management on the best practices to improve the implementation of effective physical security measures.

1.6.3 Research Questions

A research question is a scientific question that a researcher wants to find answers to as part of the project they are working on (Bell, Bryman & Harley, 2022). To achieve the objectives of the study, the following research questions were formulated:

- What is the current state of physical security measures at GPW?
- What are some of the strengths and weaknesses of the physical security measures at GPW?
- What recommendations can be made to improve the effective implementation of physical security measures at the GPW?

1.7 Overview of the Research Methodological Framework

The study used an exploratory research design to explore people’s thoughts. The exploratory research design was chosen because it gave the researcher a better idea of how the people who took part in the study felt about different aspects of physical security at GPW. Doabler, Fien, Nelson-Walker, and Baker (2012) and Creswell (2016) note that exploratory research is used to obtain background information to help identify unknown aspects. Neumann (2014) says exploratory research involves diving into a new topic to pose questions for future research, and it helps researchers acquire as much information as possible. According to Neumann (2014), an exploratory inquiry helps learn facts, fundamental issues, and the context of a problem. For this study, the researcher employed the qualitative research methodology. The technique of convenience sampling was used to collect data from the participants. As a research tool, semi-structured interviews were conducted, and an interview guide was used to guide the interview process. Chapter 3 provides the details of the research methods applied in the study.

1.8 Value of the Study

The study added value to several people or organisations in different ways. The researcher benefited through academic achievement and personal knowledge development. Apart from the researcher's benefit, the GPW benefited from this research since they can integrate the study findings into their security systems planning and implementation. In this way, the organisation can enhance its capacity and thus improve the effectiveness of the current physical security measures.

The University of South Africa (Unisa) will also benefit from this study since the researcher will write an article based on the research to be published in an accredited journal. This qualification will also increase the number of graduates at Unisa, demonstrating an increase in graduation output. The community and GPW clients will gain through improved security measures and, in this way, reduce their fear of becoming a victim of crime during visits to the GPW or of receiving false face-value documents.

1.9 Outline of the Dissertation

Chapter 1: Introduction and general orientation

The chapter discusses the background of the study, problem statement, research aim and objectives, research questions, and critical theoretical concepts.

Chapter 2: Literature Review

This chapter provides an overview of the literature on physical security measures and their application in similar organisations. The chapter also discusses international literature on the effectiveness of physical security measures at similar organisations.

Chapter 3: Research design and methodology

This chapter discusses the research design and approach, population and sampling techniques, and unit of analysis. It also discussed the data collection method and data analysis. Ethical considerations and trustworthiness are also discussed in this chapter.

Chapter 4: Discussion and interpretation of findings

This chapter presents the analysis of research findings as emanated from the interviews with the participants.

Chapter 5: Conclusions and Recommendations

The purpose of this chapter is to summarise the main conclusions and suggest recommendations to improve the effectiveness of physical security measures at the GPW.

1.10 Conclusion

The chapter introduced the context of the study that intended to examine the efficacy of physical security measures at the GPW. The chapter introduced security breaches, such as unauthorised access to secure government buildings. The chapter gave the background on how physical security effectiveness is relevant to strategic organisations, including GPW. In addition to providing the study's rationale, the chapter explained the study's significance to academics, the GPW, and other organisations. The problem observed at GPW was found on Closed-Circuit Television (CCTV), surveillance cameras, security guards, alarm systems, walkthrough detectors, scanners, and automatic security gates. Key terms defined after finding relevance to the study include access control, physical security controls, physical security, procedural control, risk, security risk management, and security breach. The chapter introduced the study as qualitative exploratory research intended to learn facts and identify fundamental issues within a specific context. The next chapter presents a literature review of the key issues in the security industry.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

According to Frank and Hatak (2014), reviewing the literature on a phenomenon is one of the critical steps in the research procedure. Reviewing the literature may also be used to reflect on accumulated knowledge as researchers learn from and build upon the work of others. Frank & Hatak (2014) identify four objectives for examining the literature. These are demonstrating familiarity with the specific body of knowledge to build credibility; identifying the methodology used in earlier studies and deciding on which research design to adopt; connecting the study to factors previously known in the field; and learning from other researchers to spark new knowledge ideas. This study used journals, government publications, academic research projects, books, and online sources such as the Internet. The internet gives access to a range of information, making it easier for a researcher to access electronic sources available on the web. This chapter provides theories that brought out the need for security. The Chapter will give the origins of security theories and highlight the relevance of such security theories to physical security measures. Since there are scarcely related studies, the chapter discusses successful cases of physical security measures of security services for government arms that deal with printing.

2.2 Government Printing Works

The GPW, based in Pretoria, is a security document printing company in South Africa. It has been printing security documents for the South African government, state-owned companies, the private sector, and some countries in Sub-Saharan Africa for more than 100 years (GPW, 2020). Passports, visas, birth certificates, identification documents, government stationery, and government gazettes are official documents printed at GPW. This department has worked hard to stay committed to secure printing to prevent fake documents, ID cards, and passports from being made, which could lead to fraud and identity theft (GPW, 2020).

The Security Services division is integral to the GPW’s operations, production, human resources, and other departments. The most important job of ensuring that the organization’s assets are safe has been given to the Security Services division, which is part of the Strategic Management branch of the organisation. The division is tasked to offer physical security, security operations, investigations, security management, threat and risk assessment, executive protection, and risk management. Specifically, the division offers security services, including closed-circuit television (CCTV), information security management, asset protection, security audits, and physical security and security training. The division is headed by the Security Service Director, whom everyone reports. This division ensures the strategic plan and related security policies and procedures are made, aligned, and implemented (GPW, 2020). At the GPW, different people with security-related qualifications are hired to execute security-related duties (GPW, 2021).

2.3 The Theoretical Models for the Security

There are several types of security in existence. Historically, the first forms of security included physical and international security (Lukas, 2015). The establishment of work health and safety as a distinct and third type of security may be attributed to the advent of the Industrial Revolution and the subsequent increase in job-related accidents. The advent of the vehicle and subsequent advancements in transportation has led to the establishment of road traffic safety measures (Smith and Brooks, 2013). According to Lukas, Hromada, and Pavlik (2016), the establishment of information security is attributed to the advent of the internet and computers. The development of the Internet was a catalyst for the establishment of cybernetic security measures.

Every security category employs a distinct model to address and mitigate security concerns. The process of establishing each type of security included pragmatic and deliberate procedures. Lukas (2016) said there is a period during which it is possible to formulate generalisations and develop the security model, which ought to be implemented across several categories of security. Within the security realm, several models exist to ensure information and systems security. Relevant to the current study, implementing physical security measures involves using distinct security measures, often referred to as barriers in the barrier model (Lukas, 2016). Barriers are crucial in facilitating the proper functioning of the organisation (Smith and Brooks, 2013). This section examines the prevailing models theoretically used to address security concerns.

2.3.1 The Security Models

Modeling is a method used to investigate and understand many aspects of reality (Lukas et al., 2016). The objective of modeling is to use an abstract of reality to analyse the dynamics of real-world phenomena and gain insights into their fundamental nature. The model, therefore, serves as a means to illustrate the primary facets of reality (Lukas, 2016). The model environment encompasses several components: verbal descriptions, graphical symbols, physical and mechanical equipment, mathematical tools, and computer languages used to construct analytics or simulation models. In contemporary times, models are mostly constructed via the use of word-based conceptual descriptions, mathematical tools, and computer systems that are equipped with appropriate programming languages (Tatomir, McDermott, Bensabat, Class, Edlmann, Taherdangkoo, and Sauter, 2018). In this literature, security models are conceptual models that include the fundamental principles of guaranteeing security for a reference object, conveyed verbally and figuratively.

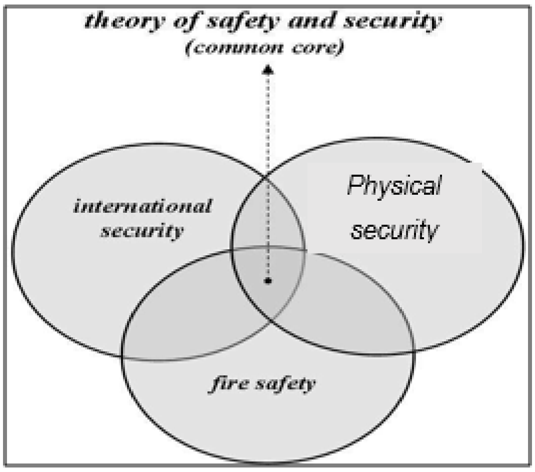
The model also incorporates security features. The security measures might be built using either logical or physical means. Among the many logical measures, one may include rules, management techniques, educational strategies, negotiating tactics, predictive models, deterrent mechanisms, encryption methods, and so on (Lukas,2016). These measurements are derived from empirical data and are used in conjunction with such data (Tatomir et al., 2018). Physical characteristics include defensive structures (e.g., fences and walls), shock-absorbing mechanisms, security personnel, tools and equipment for protection, warning and alarm systems, and supplies and resources (Lukas et al., 2016). Included among the fundamental security models are (Lukas e t al 2016):

- Regime security model,
- Proactive security model,
- Barrier security model,
- Preparedness security model,
- Reactive security model.

The security field encompasses a range of models that serve as the foundation for ensuring safety (Boustras and Waring, 2020). These models are characterized by various types and approaches, resulting in a diverse array of sub-models. Multiple security models are employed to guarantee a specific type of security (Tatomir et al., 2018). For instance, physical security, which pertains to property protection, is typically upheld through implementing measures aligned with the regime, barrier, and reactive models (Collins, 2022). The promising theory of security may derive insights from this body of information. The formulation of the security theory may be approached via several methodologies based on types of security.

The security theory is built via generalisation and induction (Leveson, 2020). Providing a theoretical framework of postulates that systematically and comprehensively elucidate security's fundamental patterns and contexts, including its vulnerabilities and protective measures, is essential. Figure 2.1 illustrates the process of generalization and induction applied to the chosen categories of security, serving as a means to develop the theory of security (Lukas, 2016).

Figure 2-1 Induction of the types of security



Source: Lukas (2016)

The theory of security has the potential to provide a comprehensive understanding of security over a wide spectrum of general features.

2.3.1.1 Regime security model

Establishing security within a regime model depends on setting norms and subsequent adherence. According to Koblentz (2013), the regime model may be characterised as a system of regulated order. Establishing these regulations delineates the boundaries within which various activities are conducted inside the corridors (McMahon and Slantchev, 2015). Rules serve the purpose of simplifying activities and ensuring the implementation of appropriate functioning styles, hence promoting security. Lukas (2016) emphasises that in the regime model, there is documentation of the process of activities and the execution of each particular action. To address these issues, it is important to possess a mechanism for detecting rule violations and the subsequent imposition of penalties (Koblentz, 2013). The norms pertaining to the state as a reference object are often published in various legal sources such as the statute book, legal code, collection of law, and other normative actions (Kagoro, 2020). Based on the regime model, the violation of established physical security regulations often incurs penalties or sanctions.

2.3.1.2 Proactive Security Model

The proactive model is founded upon a proactive attitude. According to Lukas et al. (2016), this model is future-oriented and aims to forecast events to mitigate harmful consequences. The prioritisation of action is emphasized above apathy and acts of the initiative. The model is founded upon management principles, including the active exploitation of information and the systematic search and monitoring of unpleasant occurrences with subsequent resolution (Chandra and Sadikin, 2020). This model, therefore, involves forecasting future events and proactively equipping the necessary resources and strategies to address forthcoming physical security challenges.

2.3.1.3 Barrier security model

Barrier models are mostly used as security models. According to Lukas et al. (2016), barrier security models are used universally in contexts where sustainable physical security is required. The presence of various measures, such as constructive and structured approaches, may often serve as a potential barrier. This measure serves as a safeguard against the establishment of a destructive relationship between two entities. Barriers may manifest physically or intellectually (Chandra and Sadikin, 2020).

The concept of a barrier is often seen in many systems to prevent or control certain elements. In addition, these systems include both technological and biological components (Peoples and Vaughan-Williams, 2020). The barrier model is recommended for all systems, irrespective of emphasis or structural layout variations.

According to Chandra, and Sadikin (2020), the principle of barriers has historically been employed in military contexts to provide perimeter protection for camps and other installations. These barriers took the form of physical structures. Barriers can also function as measures that safeguard against attacks through their effects (Peoples and Vaughan-Williams, 2020). In contemporary times, medicine has also adopted this principle in therapeutic practices, such as vaccination against epidemics. Barriers provide permanent protection, detection, and separation (Lukas et al., 2019). The objective of separation is to filter based on specific criteria. The classification of barrier models is contingent upon the desired level of protection and the preferred method of securing the barrier (Lukas et al., 2016).

According to Lukas (2016), physical security is an exemplary type of security that protects property, information, and other assets using physical barriers. Typically, it encompasses a collection of strategies aimed at reducing negative consequences. An illustration of security measures used in physical security includes implementing retention, reduction, detection, deterrent, and response (detention) strategies (Sedjelmaci, Brahmi, Ansari, & Rehmani, 2019). As such, attaining security in many domains necessitates the implementation of regular activities conducted by designated authorities using certain methods and instruments.

2.3.1.4 Preparedness security model

The concept of a reference object may be used to address anticipated security disruptions (Lukas et al., 2016). The system should include certain capabilities and possibilities that may be used to effectively manage and mitigate adverse impacts while also ensuring the security of the reference model (Saban, Rau, and Wood, 2021). Therefore, the preparation model encompasses a range of strategies and measures to ensure the security and readiness of various areas of preparedness. In the context of the readiness paradigm, security measures refer to established truths or realities that are precisely implemented. Security measures include various elements such as forces, means, knowledge, and procedures, all of which contribute to the preparedness and effectiveness of safeguarding a reference object (Saba et al., 2021).

2.3.1.5 Reactive Security Model

The reactive model is founded upon the principles of the reactive approach, which is predicated on the response to an initiating event (Lukas et al., 2016). The reaction to disruption is elicited by external pressures and mechanisms that have been contractually established (Hyder and Ismail, 2021). In many scenarios, it is deemed ineffective for every threatened entity to possess dedicated and ongoing resources and strategies to ensure security. These troops and methods are allocated for imminent security disturbance amid such disruption (Lukas et al. 2016).

Using a reactive model, we can effectively address the issue of security interruptions, which often exhibit a random nature. Security interruptions will likely be moderately elevated, including traffic accidents, fires, violent crimes, and robberies (McCrie, 2021). The model is predicated on the detection of security disruptions and the subsequent deployment of troops to address the emergency effectively. The principle behind this assertion is that perpetual security is unattainable (Hyder and Ismail, 2021). The monitoring system of interruption actively monitors various circumstances and, when necessary, deploys troops to intervene and ensure safety. The concept of the reference object is predicated upon external influences, such as the Integrated Rescue System (Sennewald and Baillie, 2020). The reactive model, therefore, encompasses reflecting on a situation, taking appropriate action, and observing the related response afterward.

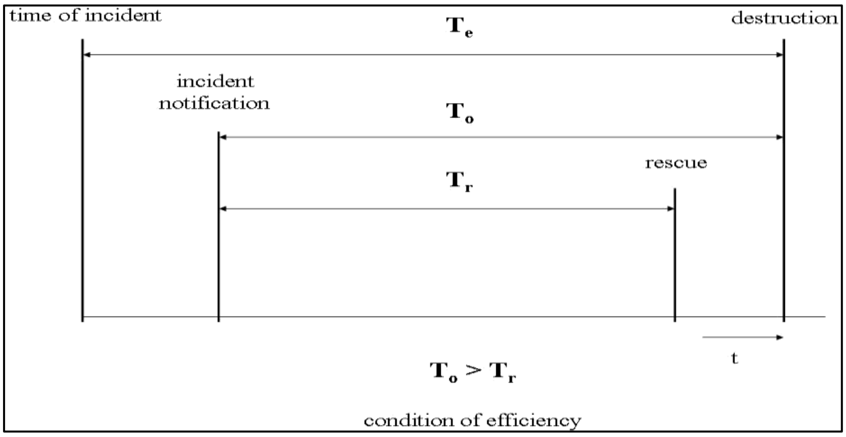
2.3.2 Reactive Model as Example of Security Model

An appropriate formal model enables the assessment of the degree of safety, security, and protection. The reactive model operates based on assisting the endangered reference object by using specialised personnel and resources strategically allocated inside a protected area (Hyder and Ismail, 2021). As mentioned earlier, the personnel can effectively carry out security, rescue, and cleaning operations at GPW. The protection system necessitates integrating communication, transportation, and protection activities (Lukas et al., 2016).

The communication system serves the purpose of receiving information about crises. Communication Technology enables the identification of security breaches and facilitates the prompt deployment of appropriate resources to the location of the emergency. The transportation system facilitates the expeditious movement of personnel and resources to the location of an emergency. The capabilities of the system include the provision of security measures, the execution of rescue missions, and the facilitation of liquidation procedures. An illustrative instance might include the police force, fire department, medical emergency response service, and privately operated security services (Lukas et al., 2016).

The fundamental characteristics of the reactive model are shown in Figure 2.1.

Figure 2-2: Basic parameters of the reactive model



Source: Lukas et al., (2016).

The figure shows that the reactive model accurately represents the tangible or conceptual components, interconnections, and characteristics. The reactive model is therefore predicated on the prompt reaction to external influences and the use of resources to mitigate a security breach. The provision of timely response has significant importance, with qualities of time and the capacity of forces and resources are crucial factors (Hyder and Ismail, 2021).

As described by Lukas et al. (2016), efficiency is quantified as the extent to which a given outcome deviates positively from the intended outcome or as a measure of the level of success attained. In the realm of technology, figuratively speaking, as well as in the domains of economics and other disciplines, the term "efficiency" refers to a dimensionless quantity that quantifies the proximity of a given process, system, or equipment to an ideal state (Charlesworth, and Pandit, 2020). Efficiency may be defined as the ratio of the measured output amount to the input quantity within a certain time frame (Chen, Huang, Li, and Wang, 2020). The optimal procedure has a level of efficiency that reaches 100% (Chen et al., 2020). An effective system of protection is defined as a system that satisfies the fundamental criterion of having a reported incident duration (To) that exceeds the response time of emergency units Tr, To > Tr (Lukas et al., 2016).

Te - The entire duration of the emergency, commencing from its inception to its conclusion, coinciding with eradicating the reference object. The temporal interval starts with the proclamation of an exceptional occurrence and culminates with the demise of the reference object (Lukas et al., 2016).

Tr - The temporal duration of the route to the occurrence's location and the responsive forces' efficacious involvement.

The effectiveness of an intervention is contingent upon the recovery of the reference object (Lukas et al., 2016). It is important to underscore that the individual time intervals are derived from the moment of event detection and subsequent reporting inside the security system (Chen et al., 2020). At this juncture, the activation of reactive forces takes place. The second argument stems from the fundamental nature of the system. In situations when detection is absent, the possibility of intervention is also absent, therefore rendering the consideration of protective measures useless. Another factor to consider is the capacity of reactive forces to respond effectively to emergencies. This pertains to the ability of reactive forces to mitigate the adverse consequences of a security breach (Lukas et al., 2016).

An illustration of a reactive model may be seen in providing physical security and property protection via private security services (Chen et al., 2020). The disruption of a protected area is a complex phenomenon involving several components, such as the guarded area, protected interests, mechanical barriers, alarm systems, intruders, and security guards. These elements interact with one another in particular ways throughout the process of disruption (Charlesworth and Pandit, 2020). Every protective system model must include distinct input and output parameters. The output parameters quantify the degree of safety provided to the item under protection. The model's input parameters are (Lukas et al., 2020):

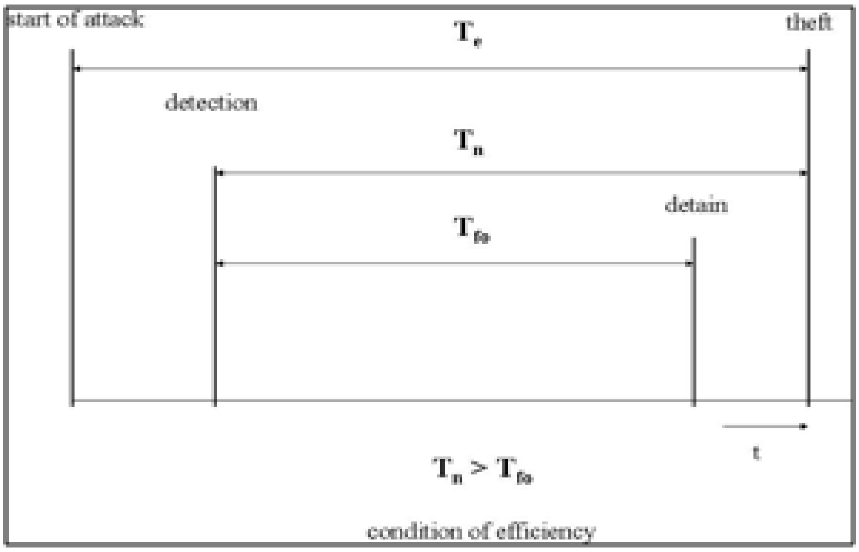
- Intention of the intruder (theft, destruction of the object, disposal technology),
- The nature and value of the protected interest (asset),
- Intruders decision-making,
- A breakthrough resistance of mechanical barriers,
- Method for the detection and evaluation of the disruption of the protected space,
- Possibilities for dividing the protected area into zones,
- Capital and operating costs relative to expected losses.

An efficient protection system satisfies the fundamental criterion of having an attack time (Tn) that exceeds the reaction time of emergency squads Tfo, ie. Tn> Tfo (Lukas e t al., 2020).

Tn - The overall duration encompassing the period from the instant of assault identification at Tdet by the detection system after departure from the safeguarded vicinity (Charlesworth and Pandit, 2020).

Tfo - The total response time of the intervention unit. Effective intervention may be defined as an intervention strategy encompassing measures aimed at detaining intruders, deterring their actions, and impairing their ability to achieve their objectives (Lukas et al., 2020).

Figure 2-3: The physical security characteristics in a reactive model



Source: Lukas et al., (2016).

Using a reactive model enables the development of an efficient protection system. Formalizing parameters enables optimizing the capabilities of forces and resources, considering the specific kind of emergency and its length. The optimization process relies on three fundamental components: communication systems, driving time, and the capacity of forces and resources (Charlesworth and Pandit, 2020; Lukas, 2016).The next section pre-empty on theoretical sources for a theory of security.

2.3.3 Theoretical Sources for a Theory of Security

Our society prioritises security; thus, resolving issues in this discipline is vital. International security, cyber security, physical security, fire safety, etc., exist today (Jarvis, 2019). The scientific research community is developing a security theory. This study examines security theory because security research nowadays has become so pragmatic. Currently, each industry does security research in its form, with each type of security usually having its professional conceptual apparatus (Peoples and Vaughan-Williams, 2020). No comparisons or generalisations were made between security types before today. Each field's experts build their security procedures. Each type of security solves its field-specific problems to avoid danger or undesirable outcomes. Each form of security was built by considering ways to make a reference object safe or secure. Different security types were explored and developed individually (Sennewald and Baillie, 2020). There is no standard security theory yet. Though there should be one unifying security theory, many disciplines have their theories. The Copenhagen School of security studies, Risk Theory, Crisis Theory, and Causality underpin and explain the origins of security theory. The next section examines how the sources mentioned above affect security theory.

2.3.2.1 Copenhagen School of Security Studies

There is a long history of theoretical security research. The major studies were on military and international security (Lukas, 2016; Sennewald and Baillie, 2020). The researchers were largely from the political science discipline, focusing on military issues between nations (Mortensgaard, 2020). The Copenhagen School of Security Studies (CSSS) was prominent in this discipline. The CSSS researched various security fields throughout the 1990s. They prioritised military, human, environmental, and other security research (Duarte and Valença, 2021). CSSS provides a conceptual security paradigm that addresses essential questions: "Whose security?" "Security of which values?" "Security against what?" The answer is a "reference object," a security-assessed item. Answering these questions also reveals the core aspects and relationships of the evaluated security. This produces situational analysis (Muraya, Okuto, Ochieng, and Gabow, 2020). The reference object threat list is another utility. The key advantages of CSSS for security research are sector definition and securitisation. A sector-based security environment deconstruction is another advantage. The new security is built to solve security that accumulates and repeats. The last advantage is securitization parameters (Muraya et al., 2020). This notion explains how the problem becomes security-related.

They specify the reference object, its protections, and its risks. This study is used to solve security issues and choose suitable physical security solutions and resources. CSSS officials stress that military security is paramount. They also advised transdisciplinary research and security solutions (Mortensgaard, 2020). The security sectors were created to solve society's security issues top-down. The CSSS benefits security theory by providing a formal security and securitization context (Lukas, 2016)

2.3.2.2 The Risk Theory as a Base for the Theory of Security

Risk theory is a popular scientific field that identifies threats, specifies risks, and describes how to overcome them (Lukas, 2016). The presence of dangers defines risk. The risk originates from intentionally managed or chaotic and uncontrolled complicated behavior (Bergström, Lundgren, and Ericson, 2019). According to Lukas (2016), the risk theory determines which threats (or bad behaviors) influence the reference object and how much they matter. As such, risk identification aims to determine the worst potential effect of threats and develop countermeasures. The security should avoid threats or negative repercussions on the reference object.

According to Lukas (2016), risk expresses how likely and big a negative influence on the reference object will be. Quantitative and qualitative risk assessments are possible. Large negative effects or damage and the likelihood of danger exposure usually define risk. Some writers include reference object vulnerability in risk definition (Bergström et al., 2019; Muraya et al., 2020). The vulnerability question is deliberate. The vulnerability highlights the reference object's risks. This parameter specifies exposition probability. If not prone to danger exposition, exposure likelihood, and susceptibility will be decreased (Lukas, 2016).

Risk management is utilized in many domains, including project management, investment, economics, and security (Zakaria, Bakar, Hassan, and Yaacob, 2019). Risk management aims to assess the negative influence on the reference objective, how it will be impacted, how it behaves, and how to minimize the effects. Risk management is crucial to security as it mainly minimises damage or impact. The risk theory might be used to specify negative repercussions that could affect the reference object. Because of this, risk management is applied in many sectors with substantial theoretical and practical progress (Lukas, 2016). Risk analysis has several forms nowadays. Depending on the methodology and application, various risk analysis methodologies may provide various conclusions when analysing security issues (Zakaria et al., 2019).

Risk management, like coercive security measures, specifies risk and reference object preparation (Lukas, 2016). Failure to identify threat sources is a drawback of risk management. Threats are accepted, and their effects are merely considered.

Adequate precautions reduce unacceptable danger (Chen and Zhu, 2019). The answer is risk acceptance, retention, transfer, and avoidance. Despite this drawback, risk theory is the source of security theory. Risk theory is useful in physical, information, and administrative security that protects reference object conditions. (Zakaria et al, 2019).

The risk theory provides a fundamental methodological framework for the study of security, including identifying and evaluating security issues via the identification of threats, risk analysis, and the selection of risk management strategies. Risk theory, therefore, provides the fundamental concepts for the philosophy of studying physical security.

2.3.2.3 The Crisis Theory and Its Relation to the Theory of Security

A crisis is a major event that harms society. The negative consequence often indicates a security breach or disaster (Lukas, 2016). It is justifiable to analyse the relationship between security and crisis theory. Crisis theory is a scientific field that studies crisis nature and causes. The crisis theory underpins crisis prevention and management. Crisis theory is dynamic and systemic (Topper and Lagadec, 2013). Crisis theory is independent of a reference object and studies crisis creation and development. The crisis theory underpins crisis management (Shrivastava, 1993).

The crisis occurs when danger arises, and the reference object's goal function is jeopardized. The crisis occurs when the reference object's circumstances change significantly (Matthijs and McNamara, 2015). Each system component's chaotic or uncoordinated behavior changes circumstances. Lack of inputs, power supply or manufacturing faults, voltage rise, etc., might cause the crisis. System adaptability demands appropriate system reactivity to each change. If changes are predicted, the system can plan and respond appropriately. The situation changes when a quick change exceeds expectations. The system may respond inappropriately in this circumstance, causing problems or crises. The situation is caused by unexpected and large negative situations and unmanaged control (Lukas, 2016). Unexpected situations cannot be foreseen. Large-scale negative events (such as natural catastrophes, stock market crashes, undiscovered computer viruses, etc.) cause problems. Unmanaged control causes the crisis as a crisis generally has latent, acute, chronic, and resolved/unresolved phases (Shrivastava, 1993).

The crisis and security theories are common scientific knowledge that provides a systematic perspective of laws, primary substantive connections, explanations, and conclusions of unique negative effects on reference objects. Crises and security events are negative repercussions (Matthijs and McNamara, 2015). Both harm the reference object. Each bad consequence has a separate cause. The crisis is caused by mismanaged control, while security incidents are caused by objective risk and purposeful, unintentional, or accidental security events.

Security breaches are disclosed when dangers exist, and exposure is purposeful, negligent, or unintentional. The disorderly development causes the security incident. It may harm and produce unfavorable interactions. The crisis is caused by uncontrolled change. Both ideas have numerous similarities but differing foundations. Security events may trigger crises and vice versa. The economic crisis increases crime, and a security event like an oil pipeline assault may produce an energy crisis (Matthijs and McNamara, 2015). The crisis theory is, therefore, intricately connected to the security philosophy by its focus on effectively handling the repercussions of breaches. As such, most security breaches include the introduction of a reference object that leads to a crisis, making it imperative to address and resolve such incidents effectively.

2.3.3.4 Causality and Its Relation to the Theory of Security

The science of causality studies cause-and-effect relationships. Causality comes from the Latin "causa" (Lukas, 2016). The cause-effect relationship is reciprocal. The law of causality states that all events have a cause and future effects. Causality describes the link between two occurrences, where one arises, and the other is the "cause" (Leveson, 2020). The reason is the phrase that creates consequence. Security theory relies on causality (Jakobsen, 2022). Causality pertains to the underlying factors that contribute to security breaches. The theory of security may include several causal factors that contribute to security breaches (Lukas, 2016). The factors at play include intentionality, carelessness, and probability. The ideas mentioned above provide novel insights and topics to security theory.

2.4 Brief Overview of the Security Industry in South Africa

South Africa's security industry is one of the biggest in the world, which may largely be attributed to rising crime rates (White, 2016). Most business owners use private security services and are starting to spend more on security because of the high incidences of crime in the country (Berg & Howell, 2017). The private security industry is worth more than R50 billion. It is expected to grow or keep growing because people, businesses, and government departments all over the country want more security (Berg & Howell, 2017).

According to the Private Security Industry Regulatory Authority (PSIRA, 2019), more than 2.3 million registered security officers and more than 498 435 are employed by just over 9 000 registered and active security businesses. According to Section 1 of the Private Security Industry Regulation Act No. 56 of 2001 (the PSIRA Act), these security businesses and security officers belong to different security service providers. Most of these security companies and officers work in Gauteng Province, where 40% are based (PSIRA, 2019).

In South Africa, the security key personnel normally constitute former army and police officers (PSIRA, 2019). The addition of ex-soldiers and police officers has also helped the security industry to grow by teaching private security organisation how to stop crime with their skills and knowledge. Because of this, more people work in the security business than in any other company in the country. There are now many more innovative and technologically advanced products for video surveillance, as well as many new ones. These systems can be used with existing security services from well-known companies. This way, assets can be better protected without spending much money on complex solutions (Atlam and Wills, 2020).

2.5 Security Measures and Security Systems

Security means protecting people, things, and information. People want to feel safe and secure, so technological advances are one of the reasons they seek security services (Low, 2017). Security companies provide services to many clients, including private businesses, government agencies, and people living in their homes (Low, 2017). Protecting people, property, and information is any security organisation's primary goal. There are two parts to security: the physical and the human. These parts, put together, make use of security measures. Security measures include equipment and people who work to improve the overall security system (e.g., a control room, guards who walk around, and guard dogs). This is considered a security measure when these are implemented and integrated. A clear security protocol, which includes procedures and operational guidelines, governs how they work independently and together (White, 2014).

Setting requirements for all physical security systems, devices, and building features is how minimum physical security standards are made (Khairallah, 2005). These rules must be followed for a new buildings, renovations, and other projects that typically need security. It is essential to do regular security surveys, inspections, and other formal risk assessments of threats and weaknesses on site (Atkin & Brooks, 2021).

On the other hand, a complete security system is in place when all security measures are working and connected (Low, 2017:367). This includes several security principles, such as layers of protection taken care of using analysis, risk assessments, risk analysis, and the creation of appropriate risk control measures. Most people think of security measures to protect against pure risks, effectively not knowing the intent for security is to create a crime-free environment (Atkin & Brooks, 2021). Therefore, the main goal of security is to figure out how vulnerable something is to risk and then use techniques and steps to bring that vulnerability and risk down to a reasonable level. In this way, security will help create a stable, reasonably predictable environment where people can move around without much trouble or risk of getting hurt (Doss et al., 2020).

Buildings are increasingly equipped with sensors and controllers, including card readers for controlling doors, thermostats, and air quality sensors feeding into the heating, ventilation, and air-conditioning system. Various electronic and mechanical components are monitored and managed by the Building Management System. At the same time, the features embedded in buildings are highly complex and diverse (Bindra & Sood, 2019; White, 2016).

2.6 Physical Security Measures

The part of security that can be seen and checked is called physical security. It is put in place as a safety measure that protects both people and property (Kriaa, Pietre-Cambacedes, Bouissou & Halgand, 2015). Notably, the highest level of protection will be given when physical security measures are implemented correctly and effectively (Perdikaris, 2014). However, it is essential to remember that physical security is only one part of an integrated security system and cannot be effective if used by itself (Kriaa et al., 2015). The goals of physical security measures are to; (a) stop an intruder from entering the premises or stop people who do not have permission from getting in; (b) detect the attempted entry or presence of an intruder if they get past the physical security barrier; (c) limit the damage that can be done if an intruder gets in without being caught; and (d) stop the intruder by using a silent alarm or calling a security patrol (Perdikaris, 2014).

Physical security measures can be put into three groups: perimeter measures on the outside, inner middle perimeter, and internal measures on the inside. The outer perimeter measures are the ones that are outside of the building. These are signs, fences, other barriers, lighting, and patrols (Al-Fedaghi & Alsumait, 2019). The inner middle ring measures are the security measures used inside the facility's walls. These include fences and other barriers, alarms (with motion detectors), CCTV external cameras, doors, locks, security staff, and access control systems (Al-Fedaghi & Alsumait, 2019). Internal physical security measures, like alarms, CCTV cameras, window and door bars, locks, protective lighting, and other barriers, can be found inside a building (Sedjelmaci, Brahmi, Ansari, & Rehmani, 2019).

The four essential security elements which must be appropriately integrated to achieve secure physical security are (Sedjelmaci e t al, 2019):

(a) Detection: Detecting and locating intruders from the protected areas. It should be noted that early detection gives the user more time for practical alarm assessment and execution of response.

(b) Assessment: Assessment is determining the cause of the alarm or recognising the activity. This must be done immediately after detection to prevent the intruder's position from being lost.

(c) Delay: Intruders must be delayed long enough to prevent them from achieving their objectives before the response force can stop them.

(d) Response: A response force must be available, equipped, and trained to prevent intruders from achieving their objectives. The response time must be less than the delay time if the response force is to intercept the intruders before they reach their goal.

In summary, a physical security system is a set of safety measures that can be used to find or stop a threat action. So, choosing a security system has costs related to the protection that make up the system, both in terms of getting and running the precautions. To select an option’s risk, one must commit resources equal to the present value of its costs (McMakin & Lundgren, 2018).

2.6.1 Biometric Technology

Hossain & Al Hasan (2022) posited that biometric technology is improving quickly and getting cheaper and better simultaneously. Biometric verification, especially fingerprint recognition, is becoming more common because it is easy to use and not too expensive. There are now many companies that sell a wide variety of biometric devices. When combined with traditional “what you have” and “what you know” methods, biometrics can become the best way to control access (Doss et al., 2020).

Most of the time, biometric identification is not used to find a match in a database of users. Instead, it is used to confirm an already established identity using a “what you have” or “what you know” method. For example, a card/PIN is used first, and then a fingerprint scan is used to confirm the result. As biometric technology improves and more people trust it, it may become the only way to prove who you are, so you would not need to carry a card or remember a password (White, 2016). Biometric access control technology decides whether or not a person may enter a building or a particular room based on the individual’s unique biometric characteristics. It mainly operates by comparing a unique fingerprint characteristic of the individual to a database containing biometric templates of authorised users. If there is a match, the individual is granted admission; otherwise, they are refused entry. Biometric technology is yet to be implemented at GPW.

The use of biometric technology yields superior results compared to the conventional methods. Biometric technology can impartially identify individuals. Impersonation will not be tolerated, and verification requirements apply to all individuals conducting attendance scans (Zywiolek et al., 2022:5). Using biometric technology has rendered roll call obsolete since these autonomous systems effectively manage attendance tracking. The advent of biometric technology enables the advantages of accessing a diverse array of employee attendance data. The risk of tampering with clocking timings is eliminated due to the real-time collection of "in" and "out" clocking data (Rohini et al., 2023:83). The biometric system remains operational even in the absence of electrical power. To ascertain personnel trends, acquiring and analyzing many reports is necessary. According to Zywiołek et al. (2022:6), the feasibility of achieving budget savings in terms of pay may be attributed to the employees' precise working hours.

However, biometric attendance technology does possess some limitations. The functionality of the biometric attendance system is contingent upon electricity availability, necessitating backup batteries to ensure uninterrupted operation. The efficacy of biometric technology can potentially undermine confidence in human capabilities. Electronic equipment can have malfunctions, and a failure rate of 1% during such malfunctions might have significant negative consequences. Using biometrics for identification may potentially encroach upon the privacy of individuals (Singh et al., 2021:15).

2.6.2 Closed-Circuit Television

According to Doss et al. (2020), closed-circuit television (CCTV) and the security room are cameras set up at entry points. As a business may have more than one way to get in, such as through the front door, the parking lot, or the back door for staff and suppliers, it is essential to keep an eye on the CCTV. At GPW, the security staff watches the CCTV cameras 24 hours a day, seven days a week. A security officer can also be in many places by sitting in front of a monitor and making decisions on the spot, like letting only authorised people into controlled areas. CCTV is a deterrent because an intruder is scared by a visible camera. On the CCTV camera, the security guard sees a break-in in progress. The CCTV then checks whether what an intrusion detection sensor said was true. Once the intruder is seen on CCTV, they are caught, and the security officer takes the person into custody (Doss et al., 2020). The implication is that CCTV is a common physical security measure that will be an effective risk management technique if properly producing intruders' pictures.

2.6.3 Alarm System

Alarm systems detect unauthorised access to a company's premises, such as a break-in when it is closed (Kamarudin, Maple, and Watson, 2019). Security cameras can detect movement and capture images of anyone who passes within range of the camera. These sophisticated, easy-to-use gadgets alert responsible parties when attackers target possessions while no one is present (Ahmad, Abdullahi, Muhammad, Saleh, & Usman, 2019). Alarms have various benefits. As it may be impractical to use security guards or personal protection around the clock, the alarm system provides protection day and night. Wireless and wired alarm systems are simple to move from one site to another. Security systems can detect fire, smoke, gas, or flooding problems (Kamarudin, Maple & Watson, 2019). However, alarm systems also have drawbacks. Sometimes, the alarm goes off for no reason. Installing wireless and hardwired alarm systems is also costly. Sophisticated burglars have been known to steal the whole alarm system if it is wireless, as they can be disconnected quickly. In addition, robbers can also easily turn off wired alarm systems (Ahmad et al., 2019). The alarm system, therefore, protects day and night because sometimes security staff or personal protection could be more practical.

2.6.4 X-Ray Machines/Scanners

An X-ray scanner detects hazardous organic, inorganic, and metallic substances, such as explosives, narcotics, drugs, and chemicals used in manufacturing drugs, radioactive substances, weapons, firearms, ammunition, knives, and blades made of metal. Various materials absorb rays at varying levels. By analysing the mass density and the atomic number of the substances of the materials that pass through the X-ray machine, security X-ray machines can detect these potentially hazardous objects (Wei, Fang, Mulligan, Chuirazzi, Fang, Wang, Ecker, Gao, Loi Cao & Huang, 2016). At GPW, there are no X-ray machines, but hand scanners are used to check for weapons by the security at the entrance. Hand scanners detect metallic and non-metallic objects, such as knives and machetes that could be used to threaten the life of people (Kamarudin et al., 2019). Scanners make security attacks more difficult, enhancing commercial property protection (Wei et al., 2016).

2.6.5 Walkthrough Detectors

Walkthrough security detectors, also known as metal detectors or security scanners, are electronic devices commonly used in public spaces such as airports, courthouses, and public buildings to detect metallic objects on a person's body, like firearms or knives (Kim, Lee & Costello, 2020). The walkthrough detector detects metal items via electromagnetic induction (Wei, Chu, Huang, Qiu & Zhao, 2020). These detectors emit a low-frequency electromagnetic field and analyze the reflected signal to identify metallic objects. However, the walkthrough detectors do not pick up other hazardous materials (Wei et al., 2020). The detector may also erroneously detect watches and small coins, embarrassing security, and the public. In addition, walk-through metal detectors may disrupt personal electronic devices like cell phones (Kim et al., 2020). This is one of the reasons that people are asked to place these items on a tray that will not pass through the detector and can be returned to the person once they have been scanned. Nevertheless, walkthrough metal detectors are a widely used and useful technology in the security field (Kamarudin et al., 2019; Kim et al., 2020). Therefore, the walkthrough security detector is a very rare physical security at organisations like GPW as the government seems hesitant to secure the security of national documents.

2.6.6 Automatic Security Gates

Security gates are automated because technology constantly improves and applies to new objects (Elechi, Ahiakwo & Shir, 2021). Some features of automatic security gates include a code-locking keypad, an intercom system, or a video camera (Elechi et al., 2021). These features make automated security gates magnificent, although they cost more than standard gates. Automated security gates at GPW allow the organisation to track visitors, especially registered vehicles. Automatic security gates are convenient for companies, but visitors must phone to gain access to the property. While this feature may deter visitors, it deters robbers (Hamid, Gee, Bahaman, Anawar, Ayob & Malek, 2018). One disadvantage of automated security gates is that they use plenty of electricity, and a loss of electricity turns off the gate. If the power goes out, a generator is therefore needed. Automated security gates are appealing, but they cost more money. The implication is that organisations can track visitors with registered cars using automated security gates. Automated security gates require much power, which disables them when there is load-shedding. Generators are essential when the electricity goes off. As such, for automatic security gates to work properly, the electricity backup should be in place to avoid intruders taking advantage of load shedding.

2.6.7 Physical protection

Physical protection provides regular and special protection through mobile patrol or fixed posts staffed by uniformed personnel hired on a contract basis. It includes security systems and devices, locking building entrances and gates outside of regular business hours, and the cooperation of local law enforcement. Depending on the location and the level of risk, a combination of these physical safeguards may also be used (Dimmick & Fennelly, 2020). “Perimeter security” is another type of physical security system applied to areas outside the security system’s control (Alguliyev, Imamverdiyev, and Sukhostat, 2018). Depending on the building and location, the perimeter of the premises may include sidewalks, parking lots, outside walls of the building, hallways, or office doors. A closed video surveillance system, lighting, and physical barriers are part of perimeter security (Alguliyev et al., 2018). At GPW, the application of physical protection has been limited to security systems and devices locking entrances after business hours. Perimeter security applicable at GPW is mainly limited to video surveillance.

2.6.8 In-house security

In-house security officers hired by the department are part of the GPW staff, complemented by other employees. This makes monitoring them easier for their in-house supervisors (Haider, Samdani, Ali, & Kamran, 2016). People also believe they communicate better if they know more about how their organisation works. They know and understand their organisation’s goals, missions, and vision; in most cases, they are dedicated and loyal security team members (Doss et al., 2020). People who work for the government tend to trust in-house security officers more because they see them as “one of their own.” They believe that security guards who work for the company are better trained, skilled, and knowledgeable about the GPW (Haider et al., 2016). Halibozek & Kovacich (2017) said that evaluating the performance of in-house security officers is essential. Supervisors should regularly meet with security officers to evaluate their performance (Doss et al., 2020). At the GPW, the in-house security meets with other sections of the GPW to identify problem areas and suggest steps to fix them to improve the security services.

Klein & Hemmens (2018) said that government departments' in-house security officers are motivated to do an excellent job because they get benefits from their employers, such as higher salaries, pension benefits, medical aid benefits, overtime pay, help with children's school, training opportunities, and chances to be promoted. Doss et al., (2020) said that security officers in government departments could do their jobs without problems or lack of resources because of how they worked. This also significantly impacts how well in-house security officers do their jobs and how happy people are (Doss et al., 2020). In-house security officers who work for the GPW security service division provide good security services because they can do their jobs in a secure environment without their contracts being cut off.

However, in-house security officers are usually not flexible when doing their jobs. For example, they often resist moving from their usual work area to a different one. Because of this, they end up doing their work unsatisfactorily (Halibozek & Kovacich, 2017). When security supervisors and managers try to do something about officers who are not doing their jobs well, the officers run to their offices for help, even when it is not necessary (Longo, Saramago, Weatherly, Rabiee, Birks, Keding & Sbizzera, 2020). Because of this, the relationship between in-house security officers who do not do their jobs well and their supervisors and managers deteriorates, which hampers the department's ability to provide good service (Longo et al., 2020).

The organisation hires security guards to work inside the building, which is usually costly. Their hiring costs include advertising, background, and criminal checks (screening and vetting processes). On the other hand, their maintenance costs include higher salaries, annual salary increases, extra benefits, ongoing training, security equipment, and uniforms (Longo et al., 220). There is evidence that the security mechanisms in place at GPW do not eliminate the possibility of security breaches within the department, so it is necessary to have in-house security officers motivated to provide effective and satisfactory service in government departments due to the benefits they receive from their employers, such as higher salaries, pension benefits, medical aid benefits, overtime payments, study help, and training opportunities (Amedzro St-Hilaire 2020; Casey 2004; Klein & Hemmens 2018; Weingart, 2000).

2.7 International Perspectives on Physical Security Systems on Government Printing Facilities

Empirical literature reviews show cases of success stories on physical security measures. Based on USA, Kenya, and Nigeria.

2.7.1 USA Government Publishing Office (GPO) Publications

In the United States of America (USA), the GPO produces and distributes information products and services for all three federal government branches, such as passports for the Department of State and the official publications of Congress, the White House, and other federal agencies in digital and print formats. The USA GPO is the federal government's official, digital, and secure resource for making, buying, indexing, authenticating, distributing, and preserving official information products (Ridge & Terway, 2019).

There is no one security standard for federal buildings because there are so many, and they are different. There is, however, a committee in charge of making standards for the security of federal buildings. Among these: The mission of the Interagency Security Committee is to protect US non-military facilities from all hazards by developing state-of-the-art security standards in collaboration with public and private homeland security partners (Hall, 2016).

Security at federal buildings is as complicated as the number of law enforcement agencies that monitor them. Different security measures can be taken to protect other buildings by the same law enforcement agency, depending on the needs of each building (Hall, 2016). This makes it hard to give complete information about threats to or problems at federal facilities. Information about threats that affect the security of federal facilities is shared between the people in charge of national facility security, the federal law enforcement agencies that protect the facilities, and the local law enforcement agencies that help the federal government. Some federal buildings, especially those without a lot of federal government, rely on state and local police forces (Longo et al., 2020).

Wiegand and magnetic stripe cards are also used in the facilities. Wiegand refers to the technology used in card readers and sensors. The card has a set of embedded wires that have been treated in a particular way and have a unique magnetic signature. When the card is swiped through the reader, the signature is picked up by a sensing coil, turning it into a string of bits. The good thing about these complicated cards is that they cannot be copied, but the bad thing is that they cannot be reprogrammed, either. With this technology, the card does not have to directly contact the reader (Longo et al., 2020).

2.7.2 British Printing Federation Ltd

British Printing Federation Ltd is responsible for printing official documents in the United Kingdom. To protect the premises, routine searching and patrolling around the premises cover both internal and external areas (Brewer, Wilford, Guelke, Hume & Moxon-Browne, 2016). Patrols are carried out regularly at unpredictable times, and the staff must have clearly defined roles and responsibilities linked to clear policies that must be followed (Wilson & Kelling, 2017). Physical barriers and other external features for extra security at the premises help prevent break-ins and unauthorised access. Controlling access to the premises includes vehicles and is an essential layer of protective security. Physical structures help prevent vehicle access. Consideration is also given to how vehicle access could be managed at the point of entry, particularly the searching or screening vehicles in response to a specific threat.

Access control systems and locks implemented at the England British Printing Federation Ltd are designed to control who can go where and when (Brewer et al., 2016). These systems integrate with physical barriers to provide delay and detection against any hostile threats. According to Wilson & Kelling (2017), controlling access is done through:

- Automatic Access Control Systems (AACS) control several doors on the premises.
- Locks (electronic or mechanical) that control access to the premises.

Furthermore, consideration is given to investing in quality access control systems that are physically robust and offer cyber security. Security control rooms form the hub of a site’s security (Campbell, 2016). The set-up of the control room allows serious incidents and crises to be handled within them without compromising the ability to deliver normal security functions. The National Police Chiefs Council, security systems policy sets out the policy requirements for alarm systems installed by compliant companies to gain police access to premises (Campbell, 2016).

2.8 Regional Perspectives on Physical Security Systems on Government Printing Facilities

We have a regional perspective on Physical Security Systems in Government Printing Facilities.

2.8.1 Nigeria Federal Government Press

The Federal Government Press is responsible for printing various documents in Nigeria, which include legal books, official gazettes, agreement papers between Nigeria and other foreign countries, reports from multiple ministries, ledger books, classified treasury books and forms, constitutional documents, laws of the federation, statutory instruments, audit reports, financial regulations, public service rules, customs tariffs, and national assembly bills. Therefore, these premises require adequate security systems (Federal Government Press, 2022). Notably, the premises have access control which encompasses primary barriers to more sophisticated infrastructure, such as biometrically restricted doors (Aladejebi & Oladimeji, 2020:41-56.).

The Nigeria Federal Government Press premises also use surveillance, including guards on patrol, burglar alarms and CCTV, and sound and movement sensors. CCTV image recognition alerts security to the arrival of people and vehicles. Facial and gait recognition is possible across the entire facility. It notifies security if an unknown person is on-site or a worker is in an area to which they should not have access (Aladejebi & Oladimeji, 2020). The facilities use magnetic stripe cards as the most common card type, with a simple magnetic strip of identifying data. When the card is swiped in a reader, the information is read and looked up in a database. While this system is inexpensive and convenient, its drawback is that it is relatively easy to duplicate the cards or to read the information stored on them (Federal Government Press, 2022).

2.8.2 Kenya Government Press

Kenya Government Press is a department that the Government Printer supervises under the office of the President, and it is in Nairobi, the capital city of Kenya. The colonial government established the Government Press Kenya in Mombasa in 1895. In 1962, the facilities were placed under the Ministry of Power and Communications, known as the Printing and Stationery Department, which was later changed to Kenya Government Press. The facilities' primary functions are printing classified government documents, revenue forms, annual, recurrent reports, bills, Acts, revised laws, stationery, and the parliamentary Hansard (Bachmann & Hönke 2010).

At Kenya Government Press, using private security guards is not new and has been propagated by the rise of terrorism in the country (Bachmann & Hönke 2010). In addition to using private security personnel, access to the premises is managed by smart cards. The facilities use smart cards, which have rapidly become the method of choice for new installations. It is a card with a built-in silicon chip for on-board data storage and computation (Kolade, Adegbile & Sarpong, 2022).

Data is exchanged with the reader by touching the chip to the reader (contact smart card) or interacting with the reader from a distance, using the same technology as proximity and vicinity cards. Smart cards offer a wide range of flexibility in access control. For example, the chip can be attached to older cards to upgrade and integrate them with pre-existing systems, or the cardholder's fingerprint can be stored on the chip for biometric verification at the card reader (Bachmann & Hönke, 2010).

2.9 The Growth of Print Security Risks

According to Lukas (2016), organizations should be aware of prevalent risks to printing security to safeguard both the company and its employees by using a secure printing solution. Once printers were connected to an organisation's IT network, they were vulnerable to the same online threats as other IoT devices, such as viruses, malware, and Distributed Denial of Service (DDoS) attacks, in which a system's resources are overloaded to make it fail (Gupta, and Dahiya, 2021). With these tools, cybercriminals can take over the machine and get full access to the sensitive company data that flows through it (Murphy, 2018). For a printer, this could mean the information from any document sent.

Also, once a hacker has control of a printer, they can use it to get into the whole business network and use it as a base to launch more attacks. In an experiment, Kolade et al. (2022) found two major flaws that let them control the printer by sending a malicious fax to the machine. Once the device was hacked, the researchers showed how to use it to get into the organisation's network.

According to Kolade et al. (2022), the increase in cloud services has opened new security risks and improved security in some ways. For example, partners can now use their cloud portals to get the latest firmware and security updates for their printer fleets, troubleshoot problems, and remotely view, manage, and set up each device. When used correctly, cloud solutions can significantly improve an organisation's security. This is why partnering with manufacturers with a well-thought-out approach to security can be crucial in helping customers build a complete security plan (Campbell, 2016).

As the number of security threats keeps increasing, business leaders will continue to look for partners who know a lot about security and can keep their data safe. The good news is that partners who show they are willing to put these needs first will reap the benefits, such as standing out in a competitive market, making customers happier, and making more money (Kolade et al., 2022).

2.10 Conclusion

The security field encompasses a range of models that serve as the foundation for ensuring security. These models are characterised by various types and approaches, resulting in diverse models. Multiple types of security models are employed to guarantee specific forms of security. For instance, physical security, which pertains to property protection, is typically upheld through implementing measures aligned with the regime, barrier, and reactive models. The most relevant to the current study is the reactive model, which is predicated on the prompt reaction to external influences and the use of resources to mitigate the occurrence of a security breach. An illustration of a reactive model may be seen in providing physical security and property protection via private security services. Using a reactive model enables the development of an efficient protection system.

The topic of security is progressively being established as a distinct and specialized discipline within the realm of science. This phenomenon eventually contributes to the advancement of its theoretical framework. An integral component of the process is the formulation of the theory of security, which subsequently facilitates the establishment of a comprehensive foundation encompassing all categories of security. The theory under discussion includes the Copenhagen School of Security Studies, Risk Theory, Crisis Theory, and Causality Theory. The emergent security theory is based upon a broadened conceptualisation derived from the existing security models. The theories mentioned above should be manifested via the formulation of postulates. The security theory uses facts and conclusions from the theories mentioned above. For instance, the theoretical framework of the Copenhagen School is founded upon a comprehensive understanding of the security landscape.

Before implementing physical security measures on any premises, it is essential to determine the potential risks and weaknesses of the present security system. Detection is of the utmost importance in physical security. While preventing all intrusions or material security breaches is nearly impossible, having the right tools to detect and deal with intrusions is essential. The literature showed that surveillance is crucial to physical security control for buildings or premises. Furthermore, securing building entrances keep intruders out and allow authorised people to access the premises. Interestingly, it is essential to note that cloud-based physical security technology is quickly becoming the favoured option for managing security over traditional on-premises systems. The following chapter provides the research methodology used in the study to achieve the objectives of this study.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

Research methodology refers to the methods and strategies used to find, select, process and analyse information regarding a particular issue (Creswell, 2016). This chapter outlines the methodology used in the study. This chapter defines the methods followed while conducting the research. This chapter examines the methodology, the research philosophy, the target population, research methods, research design, sample size, research instrument used in this study, how data was analysed, and ethical measures were applied.

3.2 Research Philosophy

According to Ryan (2018), a research philosophy is a framework that dictates how the research will be conducted. Research philosophy is a collection of theories and traditions underpinning the methodology (Bell et al., 2022; Creswell, 2016). In layperson's terms, research philosophy is a set of beliefs or assumptions used to generate and analyse information about a research phenomenon. A researcher can follow a variety of philosophies when conducting research, such as realism, interpretivism, pragmatism, or positivism (Saunders, Lewis & Thornhill, 2009).

For this study, the researcher applied the interpretivism philosophy because it is associated with qualitative techniques to understand human experience (Creswell, 2016). Using this philosophy, the researcher in this study interprets the views and opinions of research participants on the existing condition of physical security measures at the GPW, their strengths, and limitations, and makes recommendations for GPW security management on best practices to improve the security of the GPW.

According to Creswell (2016), the interpretivism perspective states that research must be conducted in natural settings to understand people's experiences. The current study supports an interpretivism research philosophy by embracing human interests in the study and highlighting that reality is socially constructed. As a result, the researcher adopts an interpretivism perspective, believing that reality is unknowable (i.e., it is a creation of an understanding and only exists in an understanding) and varies depending on the participant's insights and experience.

3.3 Research Approach

The research approach incorporates various tools, techniques, procedures, or processes to collect or review data or information. Three research approaches exist: quantitative, qualitative, and mixed (Saunders et al., 2009). Qualitative research is characterised by researchers depending on participants' input, employing open-ended questions, and collecting worded replies from respondents. The subsequent analysis involves the identification and interpretation of themes in a subjective manner (Creswell, 2016). According to Yin (2016), the qualitative research approach primarily involves the examination of individuals' daily experiences within their natural environments.

In contrast, the quantitative approach refers to a study strategy wherein data collection is structured to be measurable, and subsequent processing primarily produces objective statistical findings (Creswell, 2016). Integrating two designs proposed by Saunders et al. (2016) is an extreme mixed-method approach. The current study used the qualitative research approach. According to Creswell (2016), a qualitative approach was suitable as the researcher depends on the respondents' subjective, open-ended, and verbal responses to questions. The qualitative research approach was used as it is ideal in exploratory studies, as it seeks answers to epistemological questions like how things came to be what they are and why something happens the way it does (Busetto, Wick & Gumbinger, 2020).

The qualitative research approach was also appropriate because the intention was to get participants' perspectives on the state of physical security at the GPW and why they have those perspectives. The qualitative research approach was chosen to determine people's thoughts about a situation (Ryan, 2018), such as the strength, weaknesses, and effectiveness of physical security measures at the GPW. The qualitative approach was, therefore, ideal because qualitative research studies people's everyday lives in a natural environment as seen through their own eyes and understanding (Creswell, 2016).

3.4 Research Design

The research design fulfills the study's objective by helping the researcher resolve the research problem. A research design is a plan that outlines the methods and strategy for gathering and analysing data (Ryan, 2018). An exploratory design was adopted for this study. According to Doabler et al. (2012), an exploratory research design is often used when gathering relevant background information regarding the study problem. Exploratory research is usually qualitative and helps identify areas yet to be closely investigated. Additionally, it offers details for further analysis (Creswell, 2016). According to Neumann (2014), the exploratory analysis comprises a researcher digging into a brand-new study area to offer answers to questions that may need to be addressed by other designs, such as the descriptive research design.

Exploratory research is often carried out when the issue needs to be better defined, has not been identified, or is unclear as to its full extent. According to Creswell (2016), it allows the researcher to compile as much information as possible on a particular subject. The exploratory design was used to get respondents' ideas and views to uncover previously unrecognised aspects of the physical security measures at the GPW that are currently in place, as well as their strengths and weaknesses, and to make recommendations for GPW security management on best practices to enhance security at the GPW. This means the present exploratory study was conducted primarily to learn more about physical security at GPW.

3.5 Target Population and Unit of Analysis

Grove, Gray & Faan (2019) define the research population as a group of elements or individuals with similar qualities and characteristics. A target population is a group of people who share a common interest with the researcher (Ryan, 2018). According to Bless (2021), the target population is a subset or entire population that a researcher plans to examine and analyse and the sample frame and conclusions generated from it. The targeted population for this study included 300 employees and management of the GPW, who comprise the study population.

According to Saunders et al. (2009), the unit of analysis refers to the individuals making up the target population. Kumar (2009) adds that the unit of analysis is the basic unit that is analysed to conclude a larger population or phenomenon. Taylor

(2017) defines the unit of analysis as the individuals being analysed in a research study. In this study, the unit of analysis includes employees and managers responsible for maintaining the security of the GPW.

3.6 Sampling

According to Ryan (2018), the sample is described as a subset of the entire population on which a researcher conducts a study. When representative, the sample has similar features to the whole population. Bless (2021) defines sampling as selecting a sizeable number of units to represent a larger group and then testing them to draw conclusions that apply to the entire population.

The researcher used convenience sampling for this study, meaning participants were chosen based on availability (Creswell, 2016). Because the researcher uses whoever is accessible, this is the quickest type of sampling. As a result, if a person is accessible, available, and willing to participate, they are included in a convenience sample (Saunders et al., 2009). For this study, the sample includes the employees and management responsible for maintaining the security of Pretoria's Government Printing Works.

In qualitative research, the number of informants is determined by the demand for information, ensuring that the research questions are addressed (Ryan, 2018). This is supported by Creswell (2016), who describes the saturation principle that claims that there is an optimal sample size beyond which no additional information will be collected. Using the principle of saturation, the researcher opted to conduct 20 interviews with open-ended questions about the nature, extent, and physical security measures at the GPW.

3.7 Research Instrument

After gaining permission from participants, primary qualitative data was acquired through semi-structured interviews using an interview guide as a research instrument (Appendix D). A semi-structured interview was used because it involves asking questions within a preset theme framework. An interview guide lists the broad subjects one intend to cover during the interview and the general questions one uses to extract answers for each theme (Bless, 2021). Through semi-structured interviews, participants may delve into potentially emotional and sensitive statements regarding security variables and their influence. According to Creswell (2016), respondents can reveal their secret emotions by responding to open-ended questions in a semi-structured interview guide developed by the researcher (see Annexure D). In this study, the first question of the interview guide elicits general demographic information. The follow-up questions mainly focus on the employees' roles, how long they have worked at GPW and their academic qualifications.

The second set of questions focuses on the respondents' opinions and perceptions of the current state of physical security measures at GPW. Participants were required to define security measures currently being used at the GPW, describe physical access control measures and security programs, and explain the use of biometric technology.

The third set of questions focuses on the strengths and weaknesses of the current physical security measures at the GPW. Most of the follow-up questions focus on the strengths and weaknesses of the following criteria used at the GPW, namely, the process of detecting and locating intruders from protected areas, determining the cause of the alarm or recognising the intruder's activity, and delaying intruders long enough to prevent them from achieving their goals at GPW.

The final set of questions focuses on the recommendations to the GPW security management on the best practices in implementing physical security measures and advises management on additional measures that could be taken to improve security at the GPW.

The semi-structured interviews were conducted with the sample at the departmental technical offices of the GPW. Ryan (2018) asserts that people who answer questions in a familiar environment feel safer and more at ease, making them more likely to give open and honest answers. Each interview took between 30 and 40 minutes. During the first few minutes, the researcher informed participants about the study. According to Bell et al. (2022), after laying the groundwork, the interview moved from general to specific questions to keep the discussion moving and maintain the participants' interest. The pre-planned questions were expanded on where the researcher wanted to explore a participant's answer in greater depth.

3.8 Pilot Study

Before conducting interviews, a pilot study was done to test the validity and accuracy of the interview guide. Participants in the pilot study did not participate in the final study. Any vagueness and discrepancies in the interview questions were identified and rectified (Bell et al., 2022). The purpose of the pilot project, a scaled-down version of the complete study, was to determine whether the interview guide could be used as a research instrument. A pilot study supports researchers in calculating the time each interview will take, organising questions to generate flow, and determining whether they are related to one another to elicit reliable and genuine responses (Ryan, 2018). As a result, three (3) employees who were not involved in the research were requested to test the questions to see whether they elicited the most crucial information required for the study. The research questions and the time frame were evaluated to determine how long the interview would take to finish. Resulting from the pilot study, the interviews were envisaged to take 30 to 40 minutes. The results from the pilot study showed that the interview guide was easy to respond to.

3.9 Analysis of Data

According to Ndungu (2017), data analysis evaluates the significance of data and excludes irrelevant information, resulting in a manageable scope of information. When conducting qualitative research, researchers are concerned with clearly characterising the data and presenting consistent themes (Ryan, 2018). Creswell (2016) asserts that the first advantage of using thematic analysis is that it helps the researcher to examine the data by grouping similar ideas into themes. According to Bell et al. (2022), thematic analysis is suitable because it enables the researcher to conduct fieldwork by focusing on notions gained from the literature review. This indicates that the multiple themes that emerge during the study analysis are consistent with the literature review. As a result of thematic analysis, the data analysis and data collection processes become intertwined (Morgan & Nica, 2020). This requires a systematic breakdown of data into more meaningful chunks.

Thematic analysis is a qualitative data analysis method that looks for overarching themes (patterns) and explores how those themes are classified. Thematic Analysis is believed to be the optimal method for any research that seeks to discover unknown insights through interpretations. Six steps making up the flow of theme analysis were conducted as explained next (Creswell, 2016; Braun and Clarke, 2021: 330)

Step 1: Familiarisation

The first step was to get to know the information collected. Before judging each piece of information, it was important to look at all the data as audio transcripts (Braun and Clarke, 2021: 335). During this step, the researcher also read and reread the secondary data collected from papers to understand what it says. After figuring out what the secondary data meant, the researcher chose manifest content as a unit of analysis based on the previously chosen keywords.

Step 2: Coding.

Coding involves detecting phrases or sentences and establishing brief labels or "codes" to describe their meaning (Braun and Clarke, 2021:336.). This includes reading each interview transcript and highlighting anything noteworthy. Data was coded after reading, with codes summarizing the data's main themes and meanings (Salem, Elkhwesky, and Ramkissoon, 2022). Coding was done using colors to separate themes and sub-themes.

Step 3: Coming up with ideas for themes

The resulting codes were evaluated, and themes were developed (Braun and Clarke, 2021: 336). Themes were broader than codes by combining many codes into a single theme.

Step 4: Examination of themes

Following step 3, the study verified that the themes provide meaningful data summaries. In this step, the study examines the data again and compares various themes. The following are some examples of inquiries that were made. Do we need anything else? Do these ideas have any basis in the data? How can we improve our themes' functionality? (Braun and Clarke, 2021: 330).

Step 5: Defining and naming themes

After settling on a handful of fundamental ideas, it was time to give each idea a proper label and explanation. Defining themes involves clearly explaining what each topic signifies and how it contributes to an overall understanding of the data (Braun and Clarke, 2021: 350). Part of the naming process was coming up with a brief, simple, understandable description.

Step 6: Reporting and Documentation

Ultimately, the study started writing a report (Braun and Clarke, 2021: 351). Each subject is often handled in the results or findings section.

The thematic analysis thus involves categorising and transcribing data into themes that match interview questions. Recorded interviews were transcribed to analyse qualitative data (Creswell, 2016). Coding was the thematic analysis's most important technical part (Morgan & Nica, 2020). Coding was not the end of the process; instead, it resulted in a narrative analysis of actions taken by the GPW as security measures; factors that respondents believe should be adopted as security measures at the GPW; the strengths and weaknesses of the current security measures at the GPW; the importance of reasonable security measures and effective security strategies; and the factors that respondents believe should be adopted as security measures at GPW. Thus, data analysis enabled the researcher to answer research questions and address the research problems.

3.10 Trustworthiness

In place of reliability and validity concepts used in quantitative research, qualitative research used trustworthiness as the basis for evaluating the worth of a study (Bell et al., 2022). Trustworthiness is vital in this study because the researcher needed to show the readers that the study was worthy of attention. Researchers use dependability, credibility, transferability, and conformability to assess the trustworthiness of research findings.

3.10.1 Credibility

According to Creswell (2016), if study results are credible, they are helpful to readers from outside the study. The researcher ensured that all data was collected and guided by the Unisa research ethics policy in establishing the standards and etiquette for producing high-quality, acceptable research results. The researcher restated facts, questioned the participants to verify accuracy during the interviews, and checked the integrity of his interpretation with the participants.

3.10.2 Transferability

According to Ryan (2018), transferability refers to the ability of research findings to be applied and adapted to different circumstances and contexts. To support transferability, the researcher documented the background, sampling, and characteristics of research participants, as well as data collecting and analysis methods, in detail.

3.10.3 Dependability

Dependability in qualitative research refers to the stability and consistency of the data collection and analysis processes over time (Bell et al., 2022). The data-gathering process was piloted with a sample of three respondents to assure dependability. This allowed for tweaks and modifications to questions to ensure that the respondents would have no difficulty answering them. The researcher also provided an audit trail of his decisions from the start of the research project to the development and reporting of findings. The audit trail needs to be described to enable others to evaluate the merits of the research for themselves (Carcary, 2020).

3.10.4 Conformability

Conformability is the neutrality or degree to which discoveries are consistent and repeatable (Polit & Beck, 2020). Ensuring conformability involves keeping an audit trail of analysis and methodological log entries. Qualitative researchers maintain meticulous records of all their judgments and analyses as they advance (Cardano, 2020). The conformability of the research is achieved by providing backup proof for any claim made and offering an inclusive report on the research methodology. This was done by storing audio recordings from participants. However, there is a caveat that such recordings must be securely stored and only accessible by authorised people such as the research supervisor.

In summary, the trustworthiness of research findings is examined using dependability, believability, transferability, and conformability. As a result, the information acquired is assumed to be reliable. Thus, the analysis method should reveal enough facts for the reader to thoroughly understand the stages of analysis and their limitations and strengths.

3.11 Limitations of the Research

Ryan (2018) states that limitations are defects or inadequacies in a study beyond the researcher’s control. The study identified methodological, general, and context/focus shortcomings. Two methodological restrictions apply to this study problem. The genuine influence (on a larger sample) could be drawn if quantitative rather than qualitative methods had been used. The second methodological limitation, linked to the first, is the unit of analysis (management and staff). The small sample size means the ideas, views, reasoning, beliefs, and thinking style do not represent the entire GPW workforce.

According to the researcher, this topic also has context-related liabilities. The first context-related constraint is using a single case, the GPW. The study’s second contextual restriction is that it only looks at the impact of physical security measures and no other type of security, limiting its general applicability to forms of security. However, the purpose was to provide the researcher with a clear picture of the influence of current physical security measures in a specific organisation, not to generalise to another type of security and organisation. The general limitation refers to the research approach, which may affect the findings if only deductive reasoning is used. Ryan (2018) suggests an inductive approach to determining the context of a qualitative study’s conclusions.

3.12 Ethical Considerations

Ethical considerations are a set of moral beliefs or values that binds people (Ryan, 2018). Ethical considerations, behavioral expectations, response coaching, and transitory problems should be considered because it is generally accepted that academic and applied research must examine ethical considerations.

3.12.1 Obtaining permission to conduct the study

Ethical issues included consent to conduct the project (Creswell, 2016). The researcher met Unisa's Ethical Requirements for Postgraduate Research Studies, and Unisa gave ethical permission to conduct the research (Appendix A). The researcher also sought and obtained permission from the GPW Human Resources Director (Appendix B).

3.12.2 Voluntary Participation

The study ensures voluntary participation. Voluntary participation is when individuals involved in research are free to exercise their choice to participate, devoid of any external influences or undue coercion (Yin, 2016). As such, all participants possess the autonomy to discontinue their participation in the study at any time without experiencing any compulsion to persist (Saunders et al., 2009). The consent form (Appendix C) was signed as part of a formal agreement that ensure voluntary participation.

3.12.2 Transparency

Researchers are ethically obligated to share and transparently convey their data, analyses, methodologies, and decision-making processes. This lets readers assess research and methods (Brennen, 2021). This is crucial when employing qualitative data, which is subjective, interpretable, and emergent. Qualitative research is frequently criticized for its unreplicability. This is because the qualitative analysis is subjective and interpretive. The researcher's conclusions and interpretations impact data gathering and analysis (Robertson, 2021). Therefore, data usage, gathering, and analysis transparency were ensured to allow others to replicate project results (Brennen, 2021). Transparency assisted in managing participant expectations and developing trust. This may help participants comprehend the study project's aim and their role, enabling informed participation decisions.

3.12.3 Ensuring that No Harm Comes to the Participants

Respondents were advised in the information letter that their participation would not cause them psychological or emotional harm. According to Saunders et al. (2009), psychological harm affects respondents' mental capacity, but emotional harm affects their feelings. The researcher remained unbiased and refrained from criticising the participants for avoiding causing psychological and emotional harm to the subjects.

3.12.4 Maintaining Confidentiality and Protecting Identities

According to Saunders et al. (2009), respondents should not be obliged to provide their identities. The researcher advised participants that their identities would not be revealed and that they were not obliged to provide their names or other identifying information. To protect participant anonymity and confidentiality, demographic information was only asked about educational level, age group, experience, occupation, and security grade

3.12.5 Compensation: Reimbursements and Incentives

Research participants are typically reimbursed for costs (Brennen, 2021). However, the study found it unsuitable for your research and the participants and recommended no compensation. Incentives are a thank-you for research participation, unlike payments. Incentives include cash, presents, gift certificates, and prize drawings. Ethical issues exist before presenting incentives to participants (Robertson, 2021). Incentives may assist in attracting researchers, but in most situations, they were unnecessary to ensure that study participants were genuine volunteers willing to engage.

3.12.6 Disseminating research findings

Researchers are often quite good at communicating with other researchers through scientific publications and presentations. Key findings should be disseminated appropriately among all relevant community groups. Many people view the appropriate distribution of research findings as an ethical obligation of researchers and research institutes. Developing a dissemination plan is a step-by-step process that starts with identifying the message and audience (Yin, 2016). Appropriate channels of communication must also be identified for target audiences. These audiences that need to be considered include study participants, other researchers, media outlets, health departments, community groups and members, and government/policymakers. Sharing research findings through thesis and article publication will open the door to many possibilities for research findings to improve practice and develop prevention measures and programs that ultimately lead to improved physical security measures for GPW and other organisations (Creswell, 2016).

In summary, the researcher met Unisa's Ethical Requirements for Postgraduate Research Studies and obtained permission from the GPW to conduct the study. Participants completed a consent form before the study to demonstrate that they had been informed of the purpose of the research, understanding that their identities would be kept confidential. The study maintained transparency in its research approach and offered no reimbursements or compensations for participation. The study will academically disseminate research findings. The study ensured that no harm would come to the participants as no negative statements were used to avoid causing psychological and emotional harm to participants.

3.13 Conclusion

Chapter 3 described how the study examined GPW’s security measures and explored respondents' perceptions about the GPW’s current state of physical security, the strengths and weaknesses of those measures, and their recommendations to security management on best practices. The chapter addressed research design, philosophy, strategy, methodology, and data collection to explain how the research was conducted. Qualitative research was preferred while using the exploratory research design. The analysis was interpretive. The chapter examined methods to maintain data credibility, dependability, conformability, and transferability during analysis, ensuring trustworthiness.

The next chapter analyses the results and offers a discussion and interpretation.

CHAPTER 4: ANALYSIS AND DISCUSSION OF FINDINGS

4.1 Introduction

This chapter analyses the data, presents the results, and interprets the data collected from semi-structured interviews. As stated in Chapter 1, the study had three objectives (see Section 1.62). The first objective was to evaluate the current physical security measures at the GPW. The second objective was to determine the strengths and weaknesses of the current physical security measures at the GPW, and the third objective was to make recommendations to the GPW management on the best practices to improve the implementation of effective physical security measures. The researcher collected data by conducting one-on-one interviews with the research participants to achieve these objectives (see section 3.7). Thematic analysis was used for analysis. When applying thematic analysis, the researcher followed a six-step procedure (see section 3.9). The first step was to get to know the information collected. The second step was coding which involves detecting phrases or sentences and establishing brief labels. The third step involves evaluating codes so to develop themes. Following step 3, the study verified that the themes provide meaningful data summaries. Step 5 involves defining and naming themes after settling on a handful of fundamental ideas. In the end, the study started the process of writing a report. Braun & Clarke (2006) created this method for qualitative studies. During the analysis, the researcher used color-coding to identify the different themes, sub-themes, and categories in the transcripts and grouped ideas and common words into themes. This analysis resulted in the following themes emerging from the study:

- The current state of security measures at GPW.
- Strengths and weaknesses of the current physical security measures at GPW.
- Training provided at GPW.
- Suggestions to improve the effective implementation of physical security measures at the GPW.

The results and interpretation of the data are presented in two sections. In Section A, the demographic profile of respondents is explained and described. Section B discusses and analyses respondents' responses to the interview questions.

4.2 Section A: Demographic Information.

Respondents were asked to provide demographic information in Section A of the interview guide (Appendix 1). Knowing the socio-demographic sampling information about respondents is essential because they provide context for the collected data. The respondents' demographic details comprise six items, namely gender, age, academic qualifications, experience, current role, and PSIRA grade.

Table 4.1: Summary of demographic details of participants

Participant number	Gender	Age	Academic qualifications	Years of experience	Current position at GPW	PSIRA Grade
1	Female	36-40	Bachelor of Arts, Disaster and Safety Management	2 years 6 months	Security Officer	B
2	Male	Older than 40	Grade 11	11 years	Security Officer	B
3	Male	Older than 40	Advanced Diploma in Security Risk Management	3 years	Supervisor	A
4	Female	Older than 40	Programme in Office Management	11 years	Security supervisor	A
5	Female	25-30	Advanced Diploma in Security Management	7 months	Security management intern	A
6	Female	36-40	Baccalaureus Technologiae: Forensic Investigation	16 years	Access control This includes Searching, Escort, Patrol, and identification	A
7	Male	Older than 40	B-Tech in Security Management	11 years	Deputy director security management	A

Participant number	Gender	Age	Academic qualifications	Years of experience	Current position at GPW	PSIRA Grade
8	Male	Older than 40	Grade 12	11 years	Security Officer	B
9	Male	31-35	Advanced Diploma in Security Management	2years	Security Officer	A
10	Male	Older than 40	Grade 12	2 years	Security Officer	A
11	Male	36-40	Diploma in Criminal Justice	2 years	Security Officer	A
12	Male	36-40	B-Tech in security management	7 months	Security Officer	A
13	Male	31-35	Grade 11	2 years	Security Officer	B
14	Female	25-30	Baccalaureus Technologiae: Forensic Investigation	5 years	Security Officer	A
15	Male	Older than 40	Grade 12	10 years	Security Officer	B
16	Male	31-35	Advanced Diploma in Security	3 years	Security Officer	A
17	Male	Older than 40	B-Tech in Security Management	11 years	Supervisor	A
18	Female	31-35	Grade 11	2 years	Security Officer	A
19	Female	31-35	Grade 12	5 years	Security Officer	B
20	Male	Older than 40	B-Tech in Security Management	10 years	Supervisor	A

4.2.1 Age and Gender of Respondents

The data shows that 13 male and 7 female participants agreed to participate in this study. The reason for having more males is that the security service industry is generally male-dominated. This is confirmed by the 2021/2022 PSIRA Annual Report, which confirms that fewer females are registered on their database, although this number is increasing slowly (PSIRA, 2022). According to age distribution statistics, the modal age (the age that appears often-9 times or 45%) was 'older than 40'. This shows that most participants were old enough to be key informants in the study.

4.2.2 Academic Qualification of Respondents

Respondents were asked to disclose their educational backgrounds to determine their organisational skill level. Data analysis revealed that 35% had Grade 12 and below, 30% had diplomas, and the remaining 35% possessed bachelor's degrees. The data shows that the targeted respondents are well-educated and have the skills to execute their daily functions.

4.2.3 Experience of Respondents

Respondents were asked to indicate their years of experience at the organisation to determine the tenure of employees. Table 4.1 shows that 25 % of respondents reported 11 years and 2 years of experience at GPW. 10 % had equally worked for seven months, 3 years, 5 years, and 10 years. 5% had equally worked for 16 years and 2 years six months. The results show that most staff have the practical experience to justify interviewing them about the current state of physical security measures at GPW. This made the study credible and justifiable in determining the strengths and weaknesses of the current physical security measures. The above distribution of years of experience further strengthens the quality of feedback received, as most participants have been in their current position for a reasonable period. The participants in this survey were familiar with the working dynamics of their organisation. They had sufficient age maturity and work experience to generate an educated view of the organisation because of the years worked at GPW and the relatively high mean age.

4.2.4 Occupational status

Respondents were required to disclose their occupational roles at work to determine their positions in security at the organisation. The data analysis regarding the respondents' occupational status shows the majority performed different functions, such as security supervisor (4), security management intern (2), access control (4), assistant director security management (1) deputy director of security management (1), director of security management (1) and security officers (50).

4.2.5 Grade

The private security sector's governing body and regulatory body is the Private Security Industry Regulatory Authority (PSIRA). PSIRA certifies and awards grades to security guards from A – E, with Grade E being the entry-level grading for beginner security guards and Grade A being the highest grading for supervisory guards (PSIRA, 2022). To determine the grade of respondents on PSIRA, they were to disclose their roles. The grades of the respondents were either Grade A or B: 70% were in Grade A, and 30% were in Grade B.

In summary, 12 male and eight female participants were included in this study. The modal age was over 40 years of age. A minority (30%) of the respondents were found to be in Grade B, and the majority (70%) were in Grade A on PSIRA. The participants in this survey had good experiences such that they were familiar with the working dynamics of GPW. The analysis of occupational status shows that the majority performed different functions, such as security supervisor, security management intern, access control, deputy director of security management, and security officer. However, most participants are working as supervisors.

4.3 Section B: Presentation of Findings

This section discusses the study's findings and analyses how they relate to the objectives. All recorded data were transcribed verbatim and subjected to the processes indicated in Chapter 3 for thematic analysis (see section 3.9). The application of thematic analysis served to make sense of the data. It required selecting, arranging, validating, analysing, and reporting on themes, sub-themes, and categories. Based on this analysis, the following key themes emerged:

- Theme 1: Current state of physical security measures at GPW.
- Theme 2: The strengths and weaknesses of the current physical security measures at GPW.
- Theme 3: Training provided at GPW, and
- Theme 4: Suggestions to improve the effective implementation of physical security measures at the GPW.

These themes are explored and analysed in the following sections.

4.3.1 Theme 1: Current state of physical security measures at GPW

The researcher asked participants the following question:

- *What is the current state of physical security measures at GPW?*

This question required respondents to express their views and opinions on the current physical security measures at GPW. The objective of physical security measures is to protect buildings and their contents. In summary, they keep undesirables out and let authorised people in (Urhiewhu et al., 2018). An excellent physical security measure is defined by its ability to protect the organisation and its employees. When one talks about security, they are talking about the ability to provide a fundamental level of protection for people, assets, and information. Recent technological advances are important in people's decisions to hire professional security guards for peace of mind (Milubi, 2020). The following shows the sentiments expressed by the respondents on the current state of physical security measures at GPW.

> Respondent 1: *"…the best…restrictions on other workstations…access control system …CCTV Cameras are in place…"*
>
> Respondent 3: "*Surveillance, security guards, protective barriers, locks, and perimeter are designed to protect persons and property.*"
>
> Respondent 4: "…*security guards … access control… metal detectors, X-ray machines … CCTV …*"
>
> Respondent 5: "*CCTV surveillance, security guards, protective barriers, locks, access control perimeter…*"

> Respondent 6: "*Access control, Surveillance, electric fence, alarm system, and identification system.*"

From these responses, the key/common security measures the respondents identified at GPW were security guards, access control, CCTV surveillance, and an alarm system. The current status of security is in line with security models. It is in line Regime Security Model by having access control that set norms and subsequent adherence. Based on the regime model, the violation of established access control as a physical security regulations attract penalties at GPW (see section 2.3.1.1). The physical security is also complying with Proactive Security model by setting up of alarm system and CCTV which are founded upon a proactive attitude and forecasting of future events and proactively equipping the necessary resources and strategies to address forthcoming physical security challenges (see section 2.3.1.2).

The physical security at GPW is also complying with Barrier Security Model as they are barriers that often manifest as physical structure such as CCTV and alarms (see 2.3.1.3). The barrier security measures can also function as measures that safeguard against attacks through their effects (Saba et al., 2021). The physical security at GPW is complying with Reactive model of security by having security guards on standby as troops allocated for imminent security disturbance amid such disruption (Lukas et al. 2016).

Despite most participants agreeing that the GPW security system comply with most of the security models such that one considered security adequate to prevent security risks from occurring at the organisation, two participants indicated that they were vulnerable and susceptible.

The following verbatim statements from respondents confirm their responses:

> Respondent 10: "*Ensure their GPW server room door is always locked. Make sure the most vulnerable devices are in that locked room. Disconnect computers that aren't being used and lock empty offices.*"

> Respondent 20: *"At most, I would characterise them as susceptible, given that the access control system, for instance, is not integrated and CCTV is operational."*

The susceptibility of physical security, such as CCTV at GPW, will likely produce black-and-white images that may not identify the intruder. Based on negative sentiment from respondent 20, the CCTV system at GPW may not effectively stop security breaches. Based on the preceding few negative sentiments, the watertight physical security framework comprises means satisfying majority of dictates of security models. The efficacy of an organization's physical security program is frequently contingent upon the effective implementation, enhancement, and upkeep of each of these model constituent elements. The negative sentiment prove the point that the physical security at GPW may need to also comply to the Preparedness security model as the security system should include certain capabilities and possibilities that may be used to effectively manage and mitigate adverse impacts while also ensuring the security of the reference object (see section 2.3.1.4). This finding is in line with Low (2017), who said that companies that provide security services sell their products to a wide variety of customers worldwide, including home customers, private organisations, and government departments. The physical environment and its people must therefore be protected to ensure security. Combining these physical security components results in creating and implementing a security measure. The current state of physical measures at GPW should combine different models in formulating its physical security model to enhance or improve their overall security system. This is also supported by Khairallah (2005), who suggested that establishing requirements for all physical security systems, present is part of developing minimum standards for physical security.

As such, results are further supported by Perdikaris (2014), who suggested that physical security measures serve several purposes: (a) preventing an intruder from entering the premises, also known as discouraging entry to people who do not have authorised access; (b) detecting the attempted entry or presence of an intruder if an intruder is successful in illegally entering premises through the physical security barrier; (c) reducing the amount of damage that can be caused if an intruder gains access without being discovered; and (d) taking the burglar into custody by activating a stealth alarm or notifying a security patrol (Amedzro St-Hilaire, 2020, Casey, 2004; Perdikaris, 2014).

The results that the physical security at GPW is better is also in line with Lukas e t al (2016) who said that if any organisation refer to a reactive model it should be able to develop an efficient protection system which necessitates integrating communication, transportation, and protection activities (see section 2.3.2).

These results are relevant in answering the research question: “What is the current state of physical security measures at GPW?” Therefore, the first objective to evaluate the current state of physical security measures at GPW is met because participants described the current state of physical security measures as best, adequate, protective, good and working, and still in good condition. The next section explore strength and weakness theme.

4.3.2 Theme 2: The Strengths and Weaknesses of the Current Physical Security Measures at GPW

4.3.2.1 Sub-theme: Strengths

Physical security is fundamentally concerned with protecting facilities, people, and property from threats. It consists of physical deterrence, detection of intruders, and a response to these threats (Ghazi, 2016). This theme was extracted from the question that elaborated on some of the strengths and weaknesses of the physical security measures implemented at GPW. This theme displays the opinions of GPW personnel regarding the strengths and weaknesses of the physical security measures implemented at GPW. The sub-themes identified are strengths and weaknesses.

The investigation then retrieved respondents’ sentiments on strengths.

> Respondent 1: “ *CCTV cameras help monitor, Alarms detect the intruders, security officers patrol, Fence wall is high enough….*”
>
> Respondent 2: *“The strength of the current security measures is CCTV can monitor and see if there are any unwanted persons in the building and yard. The perimeter wall cannot be easily climbed, and an electric fence will deter criminals; motion detectors will detect unwanted intruders. Alarm system…”*
>
> Respondent 3: *“With the current access control system, we can get access event report for every employee to track and trace their movement. With CCTV*

> *cameras, we can get pictures and videos and act immediately to prevent theft or damage to property and information and when needed for evidence. Using an X-ray machine, we can identify unwanted objects such as weapons, alcohol, or office assets whenever we scan the bags/containers…."*
>
> Respondent 15: *"Strengths: Communication, teamwork, and leadership abilities…."*

The respondents listed many strengths of the current physical security measures at GPW. CCTV cameras, alarms, security officers, fence walls, motion detectors, X-Ray machines, leadership skills, communication, and teamwork are all required to make an excellent physical security measure. It was also good to discover that the respondents mentioned leadership skills, communication, and teamwork as strengths of a good physical security measure. Despite having all the other measures, a good leader who communicates and pushes for cooperation always makes executing a specific order in security easy. This shows that the current system works well, although several weaknesses are explored in the next sub-theme. Like in the previous theme there are so many strength of the physical security at GPW which resonates well with models that underpins the adequacy of physical security measures.

The results are in line with Lukas e t al (2016), who included among the fundamental security models are regime, preparedness, barrier security and reactive security models. Though the results shows lack of preparedness attitude at GPW, results shows greater strength of GPW physical security which then goes in line with Lukas e t al (2016), who said minimum physical characteristics include defensive structures (e.g., fences and walls), shock-absorbing mechanisms, security personnel, tools and equipment for protection, warning and alarm systems, and supplies and resources. .

Albeit lack of full preparedness attitude at GPW, the strength mentioned here met the minimum standards for physical security at GPW, which says that a good security system is when the physical security measures become operational and connected (Lukas, 2016). The security system must include several security concepts, such as the placement of lights and protective layers, among other things. This is also supported by Atkin and Brooks (2021), who suggested that people consider a good security measure to be a means of offering appropriate levels of protection against real risk and dangers. The next section explore weaknesses of GPW physical security.

- Sub-theme: Weaknesses

It was discernible from the analysis of data that respondents raised issues relating to the weakness of current security measures at GPW. The investigation retrieved respondents' sentiments on weaknesses.

> Respondent 1: "*…There is a poor maintenance plan of the systems, Poor performing security officers, and non-functional electrical top fence".*
>
> Respondent 2: *"…Weaknesses are that security officers deployed at the gates are not consistent with their duties, today they search, and tomorrow they do not. Some of the security personnel are not properly trained to operate the CCTV. When there is a shortage of personnel, other areas of the buildings and the gates are not adequately filled with security. Some measures, such as CCTV, become off for longer when there is load shedding. X-ray and walkthrough metal becomes broken at the time and requires repairs."*
>
> Respondent 4: *"…Weakness- Fire escape door, Trouble with the delegation and lack of communication, Misuse of government properties."*
>
> Respondent 12: *"On the weaknesses, no firearms offered to security personnel on NKP buildings, patrols are taken without informing control room, security team not wearing protective combat gears, no alarm response from armed response service…."*

The majority of the respondents expressed views on the weaknesses in the physical security measures at GPW regarding a poor maintenance plan, poor performing security officers, non-functional electrical fences, lack of training, CCTV being off for long periods when there was load shedding, a shortage of security officers, lack of communication, misuse of government property, no firearms offered to security personnel and a lack of combative gear. This, indeed, makes any security system weak. The second objective to evaluate the strengths and weaknesses of the current physical security measures at GPW is met because the physical measures mentioned above describe the current state of security at GPW.

The weakness found here shows that having a water tight security at organisation is an endless journey. This is supported by Amedzro St-Hilaire (2020), who suggested that people consider a good security measure to be a means of offering appropriate levels of protection against all types of risks. The results therefore goes in line with the fact that risk theory is directly related to security theory (see section2.3.2.2). As such it is always appropriate to construct premises or locations free of criminal activity. This because the primary purpose of evaluating a security system is to determine how vulnerable something is to risk and then to put strategies and safeguards in place that will bring the vulnerability and risk down to acceptable levels. Therefore, security will help create a stable and predictable environment where people can move freely with minimal or no chance of experiencing any disturbance or injury.

The results agree to the fact that the company should always check for any security threats, prepare and proactively deals with some weakness. This is obviously because weaknesses, despite visible strength, can put customers, employees, and property at risk of several threats, which can, in turn, jeopardize the organisation’s reputation. This is supported by Khanyile (2020), who find that the Department of Basic Education criticised exam paper leakages at the GPW as a severe physical security weakness despite GPW having tight in-house security. GPW has implored to employ In-house security officers who are motivated to provide effective and satisfactory service in government departments due to benefits that they receive from their employers, such as higher salaries, pension benefits, medical aid benefits, overtime payments, study assistance, and training opportunities. These results are relevant in answering the research question: “What are some of the strengths and weaknesses of the physical security measures at GPW?”

4.3.3 Theme 3: Training provided at GPW.

Respondents were asked to provide their views on the following question:

- *What types of security training GPW offers to staff responsible for implementing physical access control measures at the organisation?*

Categories included various security training courses; firearm training; training on the security of national key points; control room operating training; access control training, computer literacy; security management and human resource management; first aid, health, and safety; service delivery services; and CCTV training courses.

Training in security awareness helps employees comprehend the potential dangers and threats posed by their systems, networks, and devices. The training ensures that staff know the possible repercussions and can protect their organization's infrastructure from external threats (Harris, 2013). Respondents were asked what types of security training the GPW offers to staff responsible for implementing physical access control measures at the organisation. The categories listed above were identified based on the responses provided by the respondents. The following are some of the verbatim responses.

> Respondent 1: *"Security refresher courses, Firearm refresher, and National key point refresher course."*
>
> Respondent 2: *"Firearm training, control room operating training, access control training, computer literacy, service delivery services."*
>
> Respondent 5: *"National key point, firefighting, first aid, crowd control."*
>
> Respondent 6: *"National key point, fire prevention, first aid, PR, health and safety, implemented by security management unit."*

Based on the respondents' responses, it can be said that GPW offers considerable training. The implication is that the security officers can perform their duties perfectly because they can get enough training to perform their tasks. Despite participants highlighting the same training being provided, Respondent 10 mentioned the Safety and Security Sector Education and Training Authority (SASSETA) skills development requirements:

> Respondent 10: *"According to SASSETA skills development, we train our officers, access and outlet control, conduct security control in areas of responsibility, and conduct evacuations and emergency drills."*

The training is intended to provide security officers in South Africa with the best skills and knowledge to protect National Key Points identified in the National Key Points Act, 1980 of the Republic of South Africa that provides for the declaration and protection of sites that are of national and strategic importance against sabotage. This is supported by researchers who suggested that training on security at National Key Points should be part of the essential training provided at the GPW (Button, 2011; Meehan and Benson, 2015; Milubi, 2020; Nalla and Gurinskaya, 2017; Tate, 1997, Yoshida, 1999).

4.3.4 Theme 4: Suggestions to improve the effective implementation of physical security measures at the GPW.

To improve the implementation of physical security measures at the GPW, respondents were asked, "What recommendations can be made to improve the effective implementation of physical security measures at the GPW?" The following are some of the categories that were derived from the responses of the participants regarding what additional measures they would think can be implemented at GPW, assuming that the security measures are not adequate for detecting and locating intruders from the protected areas:

Physical security measures such as.

- Guard stationed inside
- Physical patrols
- Employee awareness
- Burglar door at the entrance of every factory
- Arm response
- Training of the security officials

Electronic security measures such as.

- CCTV cameras in vulnerable exit and entry points
- A maintenance plan for all the systems, e.g., Passive infrared motion and motion zones of beams
- Installation of alarm in the exam printing center
- Glass break detectors
- Security Alarms Systems can be installed inside the buildings with a motion sensor.
- Effective electric fence
- X-ray machines at all staff entrances and exits
- Visitors Management System
- Vehicles license disc and driver's license scanner
- Intercom
- Warning devices
- Active infrared beams

To increase the effectiveness of the physical security measures now in place at the GPW, additional security measures can be implemented to improve the efficiency with which they are currently being used. These electronic and physical security measures might be of great assistance to GPW in its efforts to improve its security.

4.4 Conclusion

This chapter analysed, assessed, and evaluated the GPW's existing physical security measures to determine their strengths and shortcomings and give suggestions to management on how to enhance them. This research has shown that physical security employment is still male-dominated in South Africa. The sample consisted of mature employees employed at the GPW for more years in the organisation. Respondents named security guards, access control, CCTV monitoring, and alarm systems as significant physical security measures available at GPW. Two individuals, however, said that security measures were weak and susceptible. Therefore, the first objective to assess the present physical security measures at GPW was satisfied since the majority defined it as adequate, protective, reasonable, functioning, and in excellent shape.

GPW’s physical security strengths and weaknesses were examined. The respondents listed various GPW physical security strengths, including CCTV cameras, alarms, security personnel, fence walls, motion detectors, X-Ray equipment, leadership, communication, and collaboration. Most of the respondents cited GPW’s physical security weaknesses as a poor maintenance plan, inferior performing security officers, non-functional electrical fences, lack of training, CCTV being off for long periods during load shedding, shortage of security officers, lack of communication, misuse of government property, no firearms for security personnel, and lack of combative gear. Therefore, the second aim to analyse the strengths and weaknesses of the present physical security measures at GPW was satisfied since the strengths and flaws listed above characterised the current state of security.

Regarding employee development, the GPW offers security refresher courses, firearms training, training on the security of National Key Points, control room operating training, access control training, computer literacy, security management unit, human resource management, first aid, health and safety, service delivery services and CCTV training. Security awareness training teaches employees about systems, networks, and device hazards. The training ensures personnel are aware of the consequences and can defend their organisation’s infrastructure from external attacks. According to respondents, GPW offers plenty of training. Because of their training, security professionals can do their jobs well. The analysis shows that GPW’s National Key Point training helps South African security professionals develop the best capabilities. GPW’s physical security measures might be improved by adding electronic and physical security measures.

The next chapter reviews the findings and summarises the results. It also provides recommendations to stakeholders and makes recommendations for future research.

CHAPTER 5: SUMMARY OF FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

5.1 Introduction

This chapter outlines the summary and conclusion and makes recommendations from the study. The chapter summarises the findings derived from scientific data analysis. The chapter clearly shows how research questions were answered. Before concluding the research, the chapter suggests areas to be explored by future research**.**

5.2 Summary of Findings

The results show that in defining physical security measures, employees expected physical security measures to ensure the physical protection of assets, facilities, equipment, personnel, and property. According to the results, employees described the physical security measures currently available at GPW as good. This shows that the employees were quite satisfied with the current physical security measures at the GPW. However, some of the employees made mention of specific physical security measures that existed instead of how they perceived them. A few highlighted that the current security systems were sound but needed improvement. The employees stated that good leadership skills were a strength in the physical security measures at the GPW, and lack of communication was a weakness in the physical security measures at GPW. The findings indicated that the current security measures at the GPW should be addressed first by upgrading the system to comply with preparedness security model.

The study found that the status of the physical security measures at GPW had specific methodological errors, shortcomings, and existing strengths. This is made abundantly clear by the respondents' responses, in which the comments provided by the GPW employees varied greatly from individual to individual. At the GPW, although the existing physical security system performed adequately based on the identified strengths, there was consensus among employees that security sector will always have an in exhaustive list of weaknesses. This is because security management is a subject of continuous improvement and is subjected to different security models like the regime, reactive proactive, preparedness, barrier security modes.

In general, it is vital to evaluate the potential risks and weaknesses of the current security system before establishing any further physical security measures on the premises. This is true regardless of the type of premises in question. Detection is of the utmost importance when it comes to physical security. Even though it is almost impossible to stop all incursions or breaches in physical security, it is essential to have the appropriate instruments to detect and respond to intrusions.

5.3 Achievement of Aim and Objectives

The study was conducted to fulfill the following research objectives:

- To evaluate the current state of physical security measures at GPW
- To determine the strengths and weaknesses of the current physical security measures at GPW
- To make recommendations to the GPW management on the best practices to improve the implementation of effective physical security measures.

To fulfill these research objectives, a qualitative research approach was used to examine the effectiveness of physical security measures at GPW. The researcher used an interview schedule consisting of open-ended questions to explore the participants' perceptions, knowledge, and experience of the effectiveness of physical security measures at GPW**.** Based on research objectives, several themes were developed during the data analysis: the state of physical security measures at GPW; strengths and weaknesses of physical security measures at GPW; training provided at GPW; and recommendations for effective implementation of physical security measures at GPW.

Research objective one on the current state of physical security was fulfilled by Theme 1, which showed that only two individuals said physical security at GPW was weak and susceptible while most respondents at GPW were generally satisfied as many described the current physical security measure as adequate, protective, reasonable, and functioning. Respondents confirmed that physical security included measures designed to protect assets, facilities, equipment, personnel, and property. Respondents named security guards, access control, CCTV, and alarm systems as physical security measures in place. The results confirmed the findings of researchers who stated that minimal physical security standards should include defining the criteria for all systems, equipment, and building aspects to serve purposes that include preventing an intruder from entering the premises, detecting attempted unauthorised entry or presence of an intruder and reducing the amount of damage that can be caused (Al-Fedagui and Alsumait, 2019; Baker and Benny, 2013; Mavroedis, Vishi and Josang, 2018; Milubi, 2020).

Research objective two was fulfilled through questions on the strengths and weaknesses of the physical security measures implemented at GPW. Most respondents cited GPW's physical security weaknesses as a poor maintenance plan, poor performing security officers, non-functional electrical fencing, lack of training, the CCTV being off for long periods during load shedding, shortage of security officers, misuse of government property, no firearms for security personnel, and a lack of combative gear. Physical security strengths included CCTV cameras, alarms, security personnel, fence walls, motion detectors, X-Ray equipment, leadership, communication, and teamwork. Security system strengths included assessing risk and implementing measures to reduce vulnerability and risks. It was noted that a competent security leader who communicates and encourages cooperation makes executing security orders easier. Weaknesses in security systems put customers, workers, and property at risk, which may damage the business's image. Although various weaknesses were revealed, the existing physical security system performed adequately based on the identified strengths. However, there was a consensus among respondents on in exhaustive list of weakness that may come by. This justifies that GPW working on continuous improvements on physical security breaches.

Research objective three was fulfilled by participants who recommended ways to improve the effective implementation of physical security measures at the GPW. It was recommended that security professionals should attend training to do their jobs well since the analysis showed that GPW's National Key Point training helps South African security professionals develop high-level capabilities. Respondents made various recommendations, including installing CCTV cameras at vulnerable exit and entry points, installing alarms in the exam paper printing centers, physical patrols, glass-breaking detectors, and training the security officials, mentioned in order of importance. CCTV camera installation recommendations were the most common, followed by physical patrols and better training of security officers. This showed that physical security measures must be enhanced to protect people, property, and physical assets from events that may cause damage or loss. The results also shows security as a dismal science which borrow from many theoretical underpinnings. 5.4 Recommendations

This research yielded two recommendations based on the results and the study constraints. Recommendations emerge from the conclusions, suggesting what is to be done, who is to do it, and how and when it is to be done, and should be justified based on findings, not just on the writer's opinion.

5.4.1 Recommendation based on the Findings

Like building blocks, the findings referred to various ways to improve physical security at GPW. It is recommended that GPW should implement the following measures:

- Integrate physical security with other security components to enhance or improve the overall security system. To increase the effectiveness of the physical security measures now in place at the GPW, additional electronic security measures could be implemented to improve the efficiency with which they are currently being used.
- Maintain the good state of CCTV cameras, alarms, security officers, fence walls, motion detectors, X-Ray machines, leadership, communication, and teamwork. Specifically, CCTV cameras must be installed in vulnerable exit and entry points.
- Offer training to security leaders so that they will have good leaders who communicate and push the execution of an integrated security system model.
- Improve maintenance plans.
- Have a backup electrical system to ensure CCTV is not off for long periods when there is load shedding.
- Work towards employing more security officers;
- Improve communication within the organisation.
- Repair or replace non-functional electrical fencing and increase the supply of firearms offered to security personnel and combative wearing gear.
- Motivate in-house security officers to provide effective and satisfactory service in government departments by offering them higher salaries, pension benefits,

medical aid benefits, overtime payments, study assistance, and training opportunities.

- Invest in training programs that teach security officials to assess risk and respond to crime safely and professionally. The GPW should retrain poorly performing security officers and offer training on security categories other than National Key Points, which is mostly offered at the organisation. These include security refresher courses, firearm training, control room operating, and CCTV operation.
- Install security alarm systems inside the buildings with motion sensors.

The following are additional recommended approaches that GPW should take to implement adequate physical security measures strategies:

- Installing an effective electric fence that delivers a brief, safe, and memorable shock creates a psychological and physical barrier.
- Installing alarm systems in the examination paper printing center and other security printing and storage centers to combat non-compliance and maintain accurate records of who comes and goes.
- Introducing physical patrols to protect property and lives and prevent and detect crime.
- Installing a vehicle management system to ensure that vehicle license discs and driver's licenses are scanned when entering and leaving the premises to eradicate possible theft of vehicles and store information about vehicles appropriately.
- Introducing employee awareness programs will help employees know their role in combating information security breaches.
- Installing X-ray machines at all staff entrances and exits to help detect potentially dangerous objects or weapons before they become a threat at the GPW.

5.4.2 Recommendation for Future Studies

The study was qualitative and could not be generalised to other government departments. It is recommended that future research use a quantitative approach to determine the effects of physical security measures on organisational performance. It is recommended that future studies use quantitative methods to draw objective inferences about physical security.

5.5 Conclusion

Identifying potential risks and weaknesses in the current security system is critical before implementing physical security measures on any premises. Detection is essential to physical security. While preventing all intrusions or physical security breaches is nearly impossible, having the right tools to detect and deal with intrusions is essential. According to the literature, surveillance is critical to physical security control for buildings with multiple entry points. Furthermore, securing building entrances keeps intruders out while allowing authorised personnel access to the premises. Interestingly, cloud-based physical security technology is quickly replacing traditional on-premises systems as the preferred option for premises technology.

As a result, a wide range of physical security measures should be implemented at the GPW. These should include signs, fences and other barriers, lighting, patrols, barrier alarms, CCTV external cameras, doors, locks, additional security staff, and access control systems. The GPW premises has multiple access points, such as the front entrance, car park, and rear entrance for staff and suppliers, so monitoring the CCTVs is required. Furthermore, adequately equipped control centers would allow a security officer to monitor all access points simultaneously and make decisions on the spot by allowing only authorised persons to enter the controlled areas at GPW.

REFERENCES

Ahmad, M.B., Abdullahi, A.A., Muhammad, A.S., Saleh, Y.B. & Usman, U.B., 2019. The various types of sensors used in the security alarm system. *International Journal of New Computer Architectures and their Applications (IJNCAA)*, *9*(2):50-59.

Ai-Phin, P.A., Abbas, H. & Kamaruddin, N. 2020. Physical security problems in local governments: A survey. *Journal of Environmental Treatment Techniques*, *8*(2):679-686.

Aladejebi, O. & Oladimeji, J.A. 2020. Appraisal of Technology Incubation Centres in South West Nigeria. *Journal of Small Business and Entrepreneurship*, *8*(1):41-56.

Al-Fedaghi, S. & Alsumait, O. 2019. Towards a conceptual foundation for physical security: A case study of it department. *International Journal of Safety and Security Engineering*, *9*(2):137-156.

Alguliyev, R., Imamverdiyev, Y. & Sukhostat, L. 2018. Cyber-physical systems and their security issues. *Computers in Industry*, *100(2)*:212-223.

Amedzro St-Hilaire, W. 2020. Strengths and weaknesses of the enterprise’s information system. *Digital Risk Governance* Springer: Cham, 21(1): 73-83.

Arogundade, O.T., Abioye, T.E. & Sanjay, M. 2020. An ontological approach to threats pattern collection and classification: a preliminary study to security management. *International Journal of Electronic Security and Digital Forensics*, *12*(3):323-335.

Atkin, B. & Brooks, A. 2021. *Total facility management*. London: CRC Press.

Atlam, H.F. and Wills, G.B., 2020. IoT security, privacy, safety and ethics. *Digital twin technologies and smart cities*, 2(3): 123-149.

Bachmann, J. & Hönke, J. 2010. Peace and security counterterrorism? The political effects of liberal interventions in Kenya. *African Affairs*, *109*(434):97-114.

Bailey, M., Doody, O. & Lyons, R. 2016. Surveying community nursing support for persons with an intellectual disability and palliative care needs. *British Journal of Learning Disabilities*, *44*(1):24-34.

Baker, P.R. & Benny, D.J. 2013. *The complete guide to physical security.* London: CRC Press.

Bell, E., Bryman, A. and Harley, B. 2022. *Business research methods*. Oxford: Oxford University Press.

Berg, J. & Howell, S. 2017. The private security complex and its regulation in Africa: Select examples from the continent. *International Journal of Comparative and Applied Criminal Justice*, *41*(4):273-286.

Bergström, E., Lundgren, M. & Ericson, Å. 2019. Revisiting information security risk management challenges: a practice perspective. *Information & Computer Security*, *27*(3):358-372.

Bindra, N. & Sood, M. 2019. Why, what, and how to measure and improve the security of networks (a snapshot of the current situation of security metrics and the way forward). *International Journal of Security and Networks*, *14*(3):158-166.

Bless, B.D. 2021. Literature review: A technique for conceptualizing management research in South Africa. In *European Conference on Research Methodology for Business and Management Studies* Academic Conferences International Limited 4(3): 259-257.

Boustras, G. & Waring, A. 2020. Towards a reconceptualization of safety and security, their interactions, and policy requirements in a 21st century context. *Safety Science*, *132* (1): 104-112.

Braun, V. and Clarke, V. 2021. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology*, *18*(3): 328-352.

Brennen, B.S. 2021. *Qualitative research methods for media studies*. London: Routledge.

Brewer, J.D., Wilford, R., Guelke, A., Hume, I. & Moxon-Browne, E. 2016. *The police, public order, and the state: Policing in Great Britain, Northern Ireland, the Irish Republic, the USA, Israel, South Africa, and China*. London: Springer.

Busetto, L., Wick, W. & Gumbinger, C. 2020. How to use and assess qualitative research methods. *Neurological Research and Practice*, *2(1)*:1-10.

Button, M., 2011. The Private Security Industry Act 2001 and the security management gap in the United Kingdom. *Security Journal*, *24*(2):118-132.

Campbell, T. 2016. Protection of systems. In *Practical Information Security Management*, *A Complete Guide to Planning and Implementation.* New York: Apress.

Carcary, M. 2020. The research audit trail: Methodological guidance for application in practice. *Electronic Journal of Business Research Methods*, *18*(2):166-177.

Cardano, M. 2020. *Defending qualitative research: Design, analysis, and textualization*. New York: Routledge.

Casey, E. 2004. Network traffic as a source of evidence: tool strengths, weaknesses, and future needs. *Digital Investigation, 1*(1):28-43.

Chandra, N.A. & Sadikin, M. 2020. ISM Application Tool, A Contribution to Address the Barrier of Information Security Management System Implementation. *Journal of Information & Communication Convergence Engineering*, *18*(1):39-48

Charlesworth, M. & Pandit, J.J. 2020. Rational performance metrics for operating theatres, principles of efficiency, and how to achieve it. *Journal of British Surgery*, *107*(2):63-69.

Chen, J. & Zhu, Q. 2019. Interdependent strategic security risk management with bounded rationality in the internet of things. *IEEE Transactions on Information Forensics and Security*, *14*(11):2958-2971.

Chen, L., Huang, Y., Li, M.J. & Wang, Y.M. 2020. Meta-frontier analysis using cross-efficiency method for performance evaluation. *European journal of operational research*, *280*(1):219-229.

Clarke, N.J. & Kuipers, M.C. 2015. *Re-centring Tshwane: Urban heritage strategies for a resilient capital*. Pretoria: Visual Books.

Collins, A. 2022. *Contemporary security studies*. Oxford: Oxford university press.

Creswell, J.W. 2016. Reflections on the MMIRA: The future of mixed methods task force report. *Journal of Mixed Methods Research, 10*(3):215-219.

Dimmick, M.R. & Fennelly, L.J.2020. Designing security and working with architects part 2. In *Handbook of Loss Prevention and Crime Prevention* (pp.5-20). Butterworth-Heinemann.

Doabler, C.T., Fien, H., Nelson-Walker, N.J. & Baker, S.K.2012. Evaluating three elementary mathematics programs for eight research-based instructional design principles. *Learning Disability Quarterly*, *35*(4):200-211.

Doss, B.D., Knopp, K., Roddy, M.K., Rothman, K., Hatch, S.G. & Rhoades, G.K. 2020. Online programs improve relationship functioning for distressed low-income couples: Results from a nationwide randomized controlled trial. *Journal of Consulting and Clinical Psychology*, *88*(4):283.

Duarte, D.E. & Valença, M.M. 2021. Securitising Covid-19? The politics of global health and the limits of the Copenhagen School. *Contexto Internacional*, *43*:235-257.

Elechi, P., Ahiakwo, C.O. & Shir, S.T. 2021. Design and implement an automated security gate system using a global system for mobile communication networks. *Journal of Network and Computer Applications*, *7*(1):1-10.

Federal Government Press. 2022. *Printing Nigerian Government documents*. Available at https://fmic.gov.ng/departments/federal-government-press/ [Accessed 12 December 2022].

Frank, H. & Hatak, I.2014. Doing a research literature review. In Fayolle, A. and Wright, M. (Eds.), *How to Get Published in the Best Entrepreneurship Journals*, Cheltenham: Edward Elgar. pp.94-117.

Ghazi, K.M. 2016. Safety and security measures in Egyptian hotels. *Journal of Association of Arab Universities for Tourism and Hospitality*, *15*(1):165-190.

Government Printing Works. 2020. *Welcome to GPW*. Available at https://www.gpwonline.co.za/ [Accessed 05 September 2022].

Government Printing Works. 2021. *Leading standards in origination and printing*. Available at https://www.gpwonline.co.za/GPWGazettes.htm [Accessed 05 September 2022].

Grove, S.K., Gray, J.R. & Faan, P.R. 2019. Understanding nursing research: *E-Book: Building an Evidence-Based Practice.* New Delhi: Elsevier.

Gupta, B.B. & Dahiya, A. 2021. *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures*. London: CRC press.

Haider, S.A., Samdani, G., Ali, M. & Kamran, M. 2016. A comparative analysis of in-house and outsourced development in the software industry. *International Journal of Computer Applications, 141*(3): pp.18-22.

Halibozek, E. & Kovacich, G.L. 2017. *The manager's handbook for corporate security: establishing and managing a successful assets protection program*. Oxford: Butterworth-Heinemann.

Hall, N.W. 2016. A catalyst for cooperation: the inter-agency standing committee and the humanitarian response to climate change. *Global Governance*, *22*:.369.

Hamid, E., Gee, L.C., Bahaman, N., Anawar, S., Ayob, Z. and Malek, A.A. 2018. Implementing intelligent automated gate system with QR Code-An IOT

System to help gate management. *International Journal of Advanced Computer Science and Applications*, 9(10):349-363

Harris, S. 2013. *Access control. In CISSP Exam Guide*. 6th edition. New York: McGraw-Hill.

Hopkin, P. 2017. *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management*. 4th edition. London: Kogan Page.

Hossain, M.A. & Al Hasan, M.A. 2022. Improving cloud data security through hybrid verification techniques based on biometrics and encryption system. *International Journal of Computers and Applications*, *44*(5):455-464.

Hyder, M.F. & Ismail, M.A. 2021. Securing control and data planes from reconnaissance attacks using distributed shadow controllers, reactive and proactive approaches. *IEEE Access*, *9* (21): 881-894.

Jakobsen, P.V. 2022. Causal theories of threat and success–Simple analytical tools making it easier to assess, formulate, and validate military strategy. *Scandinavian journal of military studies*, *5*(1).

Jarvis, L., 2019. Toward a vernacular security studies: Origins, interlocutors, contributions, and challenges. *International Studies Review*, *21*(1):107-126.

Jore, S.H. 2019. The conceptual and scientific demarcation of security in contrast to safety. *European Journal of Security Research*, *19*(4):157-174.

Kagoro, J. 2020. The crime preventers scheme: A community policing initiative for regime security in Uganda. In *Co-operation, Contestation and Complexity in Peacebuilding* (pp. 40-55). Routledge.

Kamarudin, M.H., Maple, C. & Watson, T. 2019. Hybrid feature selection technique for the intrusion detection system. *International Journal of High-Performance Computing and Networking*, *13*(2):232-240.

Khairallah, M. 2005. *Physical security systems handbook: The design and implementation of electronic security systems*. Oxford: Butterworth-Heinemann.

Khanyile, A., 2020. *Government Printing Works lashed for being a source of matric exam leak*. Available at https://www.iol.co.za/news/politics/government-printing-works-lashed-for-being-source-of-matric-exam-leak-37bb1dae-6bdb-4eec-b216-649bcb8bc438 [Accessed 12 November 2022].

Kim, C., Lee, K.C. & Costello, F.J. 2020. The intention of passengers towards repeat use of biometric security for sustainable airport management. *Sustainability*, *12*(11): 1-18.

Klein, M.S. & Hemmens, C. 2018. Public regulation of private security: A statutory analysis of state regulation of security guards. *Criminal Justice Policy Review*, *29*(9):891-908.

Kliman, A., 2015. The Great Recession and Marx's Crisis Theory. *American Journal of Economics and Sociology*, *74*(2):236-277.

Koblentz, G.D. 2013. Regime security: A new theory for understanding the proliferation of chemical and biological weapons. *Contemporary Security Policy*, *34*(3):501-525.

Kolade, O., Adegbile, A. & Sarpong, D. 2022. Can university-industry-government collaborations drive a 3-D printing revolution in Africa? A triple helix model of technological leapfrogging in additive manufacturing. *Technology in Society*, *69* (10):29-60.

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M. & Halgand, Y. 2015. A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety*, *139(1)*:156-178.

Kumar, A.C. 2009. Analysis of unsupervised dimensionality reduction techniques. *Computer Science and Information Systems*, *6*(2):217-227.

Landoll, D.J. 2011. *The security risk assessment handbook: AA complete guide for performing security risk assessments.* London: CRC Press.

Leveson, N., 2020. *Safety and security are two sides of the same coin*. *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice*. Cambridge: MIT.

Lewis, T.G. 2019. *Critical infrastructure protection in homeland security: defending a networked nation*. London: John Wiley & Sons.

Longo, F., Saramago, P., Weatherly, H., Rabiee, P., Birks, Y., Keding, A. & Sbizzera, I. 2020. Cost-effectiveness of in-house versus contracted-out vision rehabilitation services in England. *Journal of Long-term Care*, *20 (20)*:118-130.

Low, S. 2017. Security at home: How private securitization practices increase state and capitalist control. *Sage Journals, 17*(3):365-381.

Lukas, L., 2016. Theoretical sources for a theory of safety and security. In *The Tenth International Conference on Emerging Security Information, Systems and Technologies, Secureware*.

Lukas, L., Hromada, M. & Pavlik, L. 2016. The key theoretical models for the safety and security ensuring. In *2016 Third International Conference on Mathematics and Computers in Sciences and in Industry (MCSI)* (pp. 61-65). IEEE.

Matthijs, M. & McNamara, K. 2015. The euro crisis' theory effect: Northern saints, southern sinners, and the demise of the Eurobond. *Journal of European integration*, *37*(2):229-245.

Mavroeidis, V., Vishi, K. & Josang, A. 2018. *A framework for data-driven physical security insider threat detection.* 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), August 28-31, 2018, Barcelona, Spain.

McCrie, R. & Lee, S. 2021. *Security operations management*. Butterworth-Heinemann.

McMahon, R.B. & Slantchev, B.L. 2015. The guardianship dilemma: Regime security through and from the armed forces. *American Political Science Review*, *109*(2):297-313.

McMakin, A.H. & Lundgren, R.E. 2018. *Risk communication: A handbook for communicating environmental, safety, and health risks*. London: John Wiley & Sons.

Meehan, B. & Benson, B.L. 2015. The occupations of regulators influence occupational regulation: Evidence from the US private security industry. *Public Choice*, *162*(1):97-117.

Milubi, T.T., 2020. *An investigation into levels of service provided by private security officers at government printing works in Tshwane* (Masters Dissertation. University of South Africa, Pretoria). Available at https://uir.unisa.ac.za/bitstream/handle/10500/27616/dissertation_milubi_tt.pdf?sequence=1&isAllowed=yMilubu[Accessed 12 November 2022].

Mohamed, R., Abas, H., Hassan, N.H. & Ismail, S.A. 2021. Systematic Literature Review: Factor for Physical Security and Access Control in Maximum Security Protection. *Open International Journal of Informatics*, *9*(1):100-108.

Morgan, D.L. & Nica, A. 2020. Iterative thematic inquiry: A new method for analysing qualitative data. *International Journal of Qualitative Methods*, *19(1)*: 1-15.

Mortensgaard, L.A. 2020. Contesting frames and (De) securitizing schemas: Bridging the Copenhagen school's framework and framing theory. *International Studies Review*, *22*(1):140-166.

Moyo, S. 2019. *Evaluating the use of CCTV surveillance systems for crime control and prevention: Selected case studies from Johannesburg and Tshwane, Gauteng*. (Masters-Dissertation. University of South Africa, Pretoria). Available at https://uir.unisa.ac.za/handle/10500/26222[Accessed 12 November 2022].

Muraya, J.K., Okuto, E., Ochieng, D.O. & Gabow, N.Y. 2020. Counter-Terrorism Measures in Selected University Campuses in Nairobi County, Kenya. *International Journal of Advances in Scientific Research and Engineering*, *6*(6):63-74

Murphy, S.P. 2018. A holistic approach to Cybersecurity starts at the top. *Frontiers of Health Services Management*, *35*(1):30-36.

Nalla, M.K. & Gurinskaya, A. 2017. Common past-different paths: Exploring state regulation of private security industry in Eastern Europe and post-Soviet republics. *International Journal of Comparative and Applied Criminal Justice*, *41*(4):305-321.

Ndungu, D.N. 2017. The effects of rewards and recognition on employee performance in public educational institutions: A case of Kenyatta University, Kenya. *Global Journal of Management and Business Research*, *17*(1):43-68.

Nemeth, C.P. 2018. *Private security: An introduction to principles and practice.* London: CRC Press.

Neumann, R., 2014. *Making political ecology*. London: Routledge.

Ochara, N.M., 2016. *What is your research problem? Discovering a research(able) problem and topic*. Available at: https://www.researchgate.net/publication/332108258_What_is_your_Research_Problem_Discovering_a_Researchable_Problem_and_Topic [Accessed 12 March 2023] [Accessed 12 November 2022].

Office of the Presidency. 2019. The critical infrastructure protection act 8 of 2019. Available at: https://www.gov.za/documents/critical-infrastructure-protection-act-8-2019-english-isixhosa-28-nov-2019-0000 [Accessed 11 March 2023].

Peoples, C. & Vaughan-Williams, N. 2020. *Critical security studies: An introduction*. London: Routledge.

Perdikaris, J. 2014. *Physical security and environmental protection*. London: CRC Press.

Polit, D. & Beck, C. 2020. *Essentials of nursing research: Appraising evidence for nursing practice*. Philadelphia: Lippincott Williams & Wilkins.

PSIRA 2019. *Annual report*. Available at: https://www.psira.co.za/dmdocuments/Annual_Report_2020.pdf [Accessed 12 March 2023].

PSIRA, 2022. *Annual report*. Available at: https://www.psira.co.za/dmdocuments/annual_report/PSIRA%20Annual%20Report%202021-2022.pdf [Accessed 12 March 2023].

Raj, M.J., Gadde, S. & Jayaraman, R. 2021. Implementing biometric access control using a fingerprint for the safety and security system of electric vehicles. In *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)* IEEE. 1684-1689.

Ridge, N.Y. & Terway, A. (Eds.). 2019. *Philanthropy in education: Diverse perspectives and global trends*. Cheltenham: Edward Elgar.

Robertson, S., 2021. Transparency, trust, and integrated assessment models: An ethical consideration for the Intergovernmental Panel on Climate Change. *Wiley Interdisciplinary Reviews: Climate Change*, *12*(1), 1-8

Ryan, G. 2018. Introduction to positivism, interpretivism, and critical theory. *Nurse researcher*, *25*(4):41-49.

Saban, K.A., Rau, S. & Wood, C.A.2021. SME executives' perceptions and the information security preparedness model. *Information & Computer Security*, *29*(2):263-282.

SABC, 2020. *Basic Education to work with the Hawks in investigating Physics Paper 2 leak*. Available at https://www.sabcnews.com/sabcnews/basic-education-to-work-with-the-hawks-in-investigating-physics-paper-2-leak/ [Accessed 12 November 2022].

Salem, I.E., Elkhwesky, Z. & Ramkissoon, H. 2022. A content analysis for government's and hotels' response to COVID-19 pandemic in Egypt. *Tourism and Hospitality Research*, *22*(1):42-59.

Saunders, M., Lewis, P. & Thornhill, A. 2009. *Research methods for business students*. Boston: Pearson Education.

Sedjelmaci, H., Brahmi, I.H., Ansari, N. & Rehmani, M.H. 2019. Cyber security framework for vehicular network based on a hierarchical game. *IEEE Transactions on Emerging Topics in Computing*, *9*(1):429-440.

Sennewald, C.A. & Baillie, C. 2020. *Effective security management*. Butterworth-Heinemann.

Shohaieb, M., Hashem, A. & Hanafy, H. 2018. Effect of physical security initiatives on supply chain performance. *International Journal of Physical Sciences Research*, *2*(1):18-35.

Shrivastava, P. 1993. Crisis theory/practice: Towards a sustainable future. *Industrial & Environmental Crisis Quarterly*, *7*(1):23-42.

Singh, G., Bhardwaj, G., Singh, S.V. and Garg, V. 2021. Biometric identification system: security and privacy concern. *Artificial intelligence for a sustainable industry 4 (2):* 245-264.

Smith, C. & Brooks, D.J., 2012. *Security science: The theory and practice of security*. Butterworth-Heinemann.

Tate, P.W. 1997. *Report on Security Industry Training: A case study of an emerging industry*. Brisbane: Australian National Training Authority.

Tatomir, A., McDermott, C., Bensabat, J., Class, H., Edlmann, K., Taherdangkoo, R. & Sauter, M. 2018. Conceptual model development using a generic Features, Events, and Processes (FEP) database for assessing the potential impact of hydraulic fracturing on groundwater aquifers. *Advances in Geosciences*, *45*:185-192.

Taylor, R.R. 2017. *Kielhofner's research in occupational therapy: Methods of inquiry for enhancing practice*. Philadelphia: FA Davis.

Topper, B. & Lagadec, P. 2013. Fractal crises–a new path for crisis theory and management. *Journal of contingencies and crisis management*, *21*(1):4-16.

Urhiewhu, L.O., Emojorho, D. & Omah, J.E. 2018. Security measures adopted to prevent theft of library resources in selected academic libraries. *International Journal of Library and Information Science*, 4(1):1-10.

Wei, H., Fang, Y., Mulligan, P., Chuirazzi, W., Fang, H.H., Wang, C., Ecker, B.R., Gao, Y., Loi, M.A., Cao, L. & Huang, J. 2016. Sensitive X-ray detectors made of methylammonium lead tribromide perovskite single crystals. *Nature Photonics*, *10*(5):333-339.

Wei, Z., Chu, S., Huang, Z., Qiu, S. & Zhao, Q., 2020. Optimization design of X-ray conveyer belt length for subway security check systems in Beijing, China. *Sustainability*, 12(5), 21-33.

Weingart, S.H., 2000, August. Physical security devices for computer subsystems: A survey of attacks and defences. In *International Workshop on Cryptographic Hardware and Embedded Systems*. Berlin: Springer. 302-317.

White, J.M. 2014. *Security risk assessment: Managing physical and operational security*. Boston: Butterworth-Heinemann.

White, J.R. 2016. *Terrorism and homeland security*. Boston: Cengage Learning.

Wilson, J.Q. & Kelling, G.L. 2017. The police and neighbourhood safety are Broken Windows. In Walker, J.T. (Ed.), *Social, Ecological and Environmental Theories of Crime*. New York: Routledge. pp. 169-178.

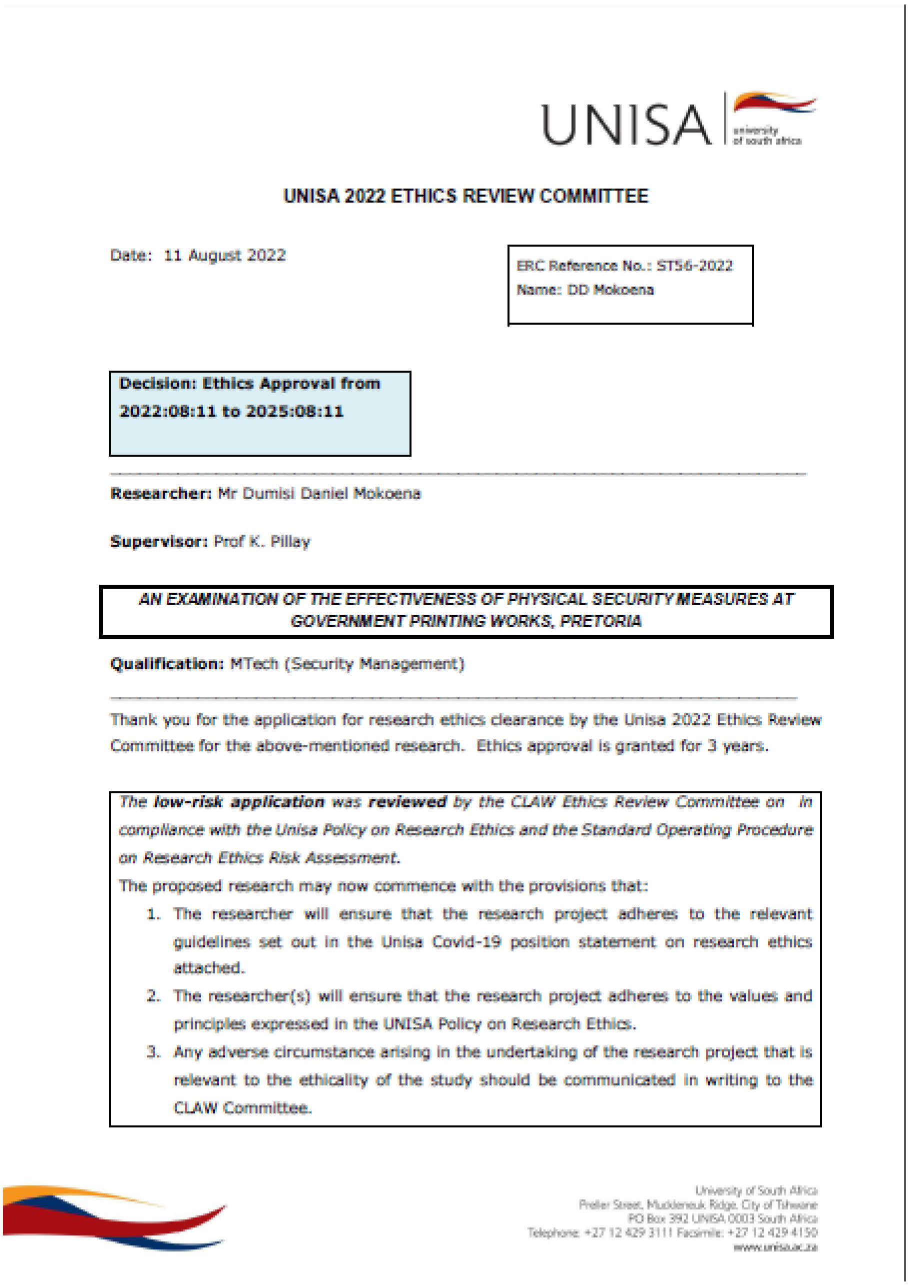
Yoshida, N., 1999. The taming of the Japanese private security industry. *Policing and Society: An International Journal*, *9*(3):241-261.

Zakaria, H., Bakar, N.A.A., Hassan, N.H. & Yaacob, S. 2019. IoT security risk management model for secured practice in healthcare environment. *Procedia Computer Science*, 161(2):1241-1248.

Żywiołek, J., Sarkar, A. & Sial, M.S. 2022, January. Biometrics as a method of employee control. In *2022 16th International Conference on Ubiquitous Information Management and Communication (IMCOM)* (pp. 1-5). IEEE.

APPENDICES

Appendix A: Ethics Approval



UNISA university of south africa

UNISA 2022 ETHICS REVIEW COMMITTEE

Date: 11 August 2022

ERC Reference No.: ST56-2022
Name: DD Mokoena

Decision: Ethics Approval from 2022:08:11 to 2025:08:11

Researcher: Mr Dumisi Daniel Mokoena

Supervisor: Prof K. Pillay

AN EXAMINATION OF THE EFFECTIVENESS OF PHYSICAL SECURITY MEASURES AT GOVERNMENT PRINTING WORKS, PRETORIA

Qualification: MTech (Security Management)

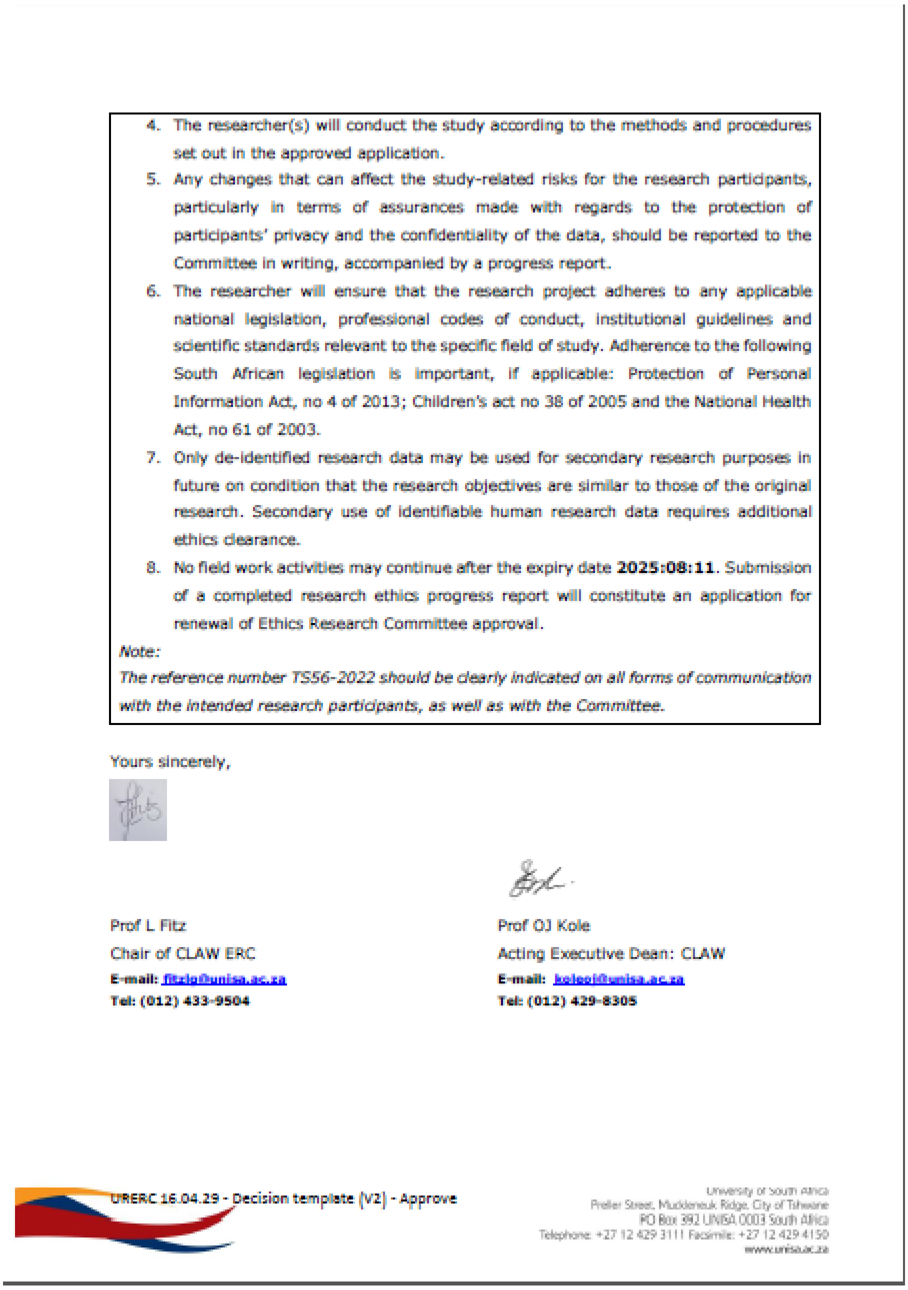
Thank you for the application for research ethics clearance by the Unisa 2022 Ethics Review Committee for the above-mentioned research. Ethics approval is granted for 3 years.

*The **low-risk application** was **reviewed** by the CLAW Ethics Review Committee on in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.*

The proposed research may now commence with the provisions that:

1. The researcher will ensure that the research project adheres to the relevant guidelines set out in the Unisa Covid-19 position statement on research ethics attached.
2. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
3. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the CLAW Committee.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za



4. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
5. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
6. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
7. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
8. No field work activities may continue after the expiry date **2025:08:11**. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:

The reference number TS56-2022 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

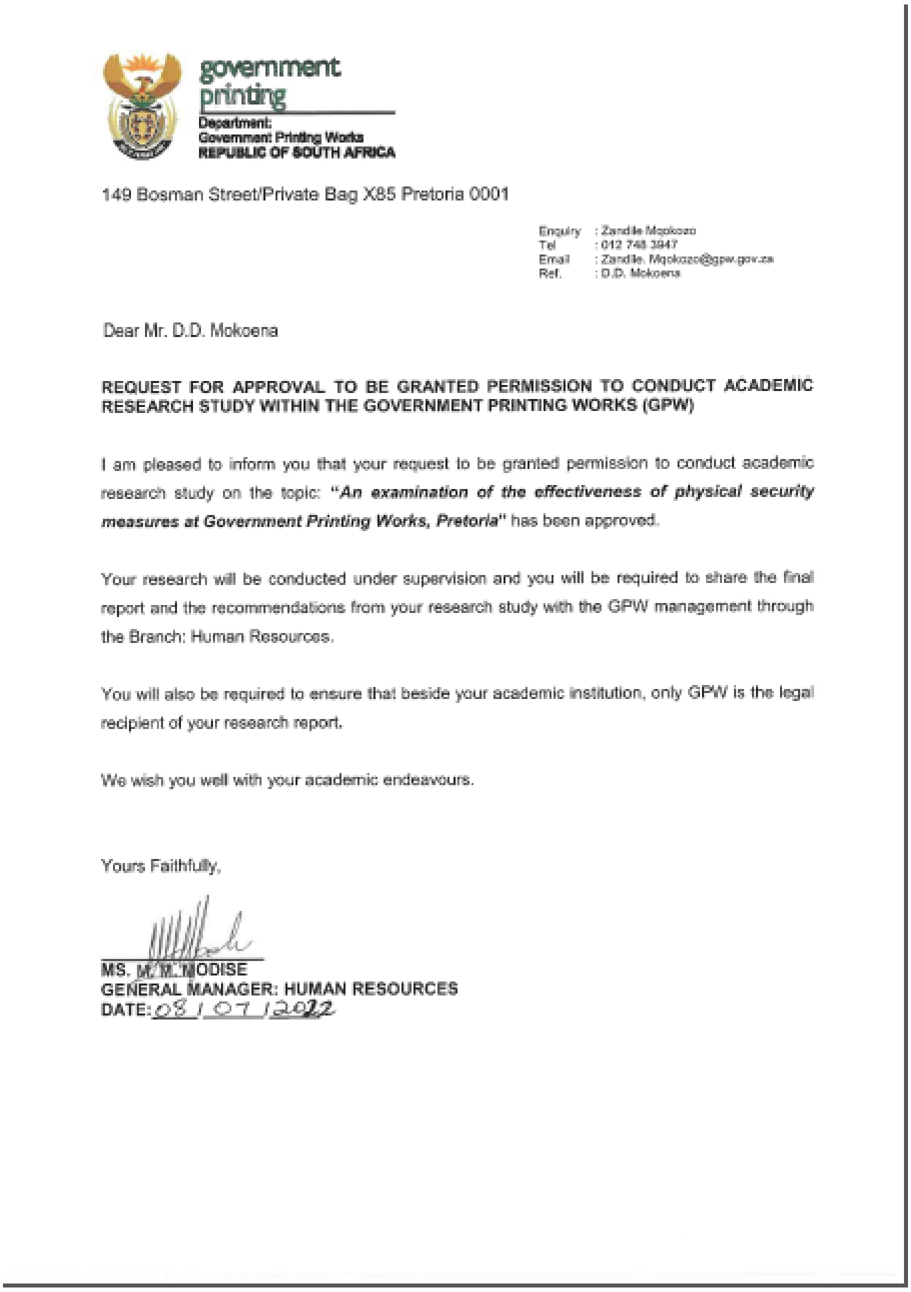
Yours sincerely,

Prof L Fitz	Prof OJ Kole
Chair of CLAW ERC	Acting Executive Dean: CLAW
E-mail: fitzlo@unisa.ac.za	**E-mail: koleoj@unisa.ac.za**
Tel: (012) 433-9504	**Tel: (012) 429-8305**

URERC 16.04.29 - Decision template (V2) - Approve

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix B: Permission to Conduct Study at GPW



government
printing
Department:
Government Printing Works
REPUBLIC OF SOUTH AFRICA

149 Bosman Street/Private Bag X85 Pretoria 0001

Enquiry : Zandile Mqokozo
Tel : 012 748 3947
Email : Zandile. Mqokozo@gpw.gov.za
Ref. : D.D. Mokoena

Dear Mr. D.D. Mokoena

REQUEST FOR APPROVAL TO BE GRANTED PERMISSION TO CONDUCT ACADEMIC RESEARCH STUDY WITHIN THE GOVERNMENT PRINTING WORKS (GPW)

I am pleased to inform you that your request to be granted permission to conduct academic research study on the topic: ***"An examination of the effectiveness of physical security measures at Government Printing Works, Pretoria"*** has been approved.

Your research will be conducted under supervision and you will be required to share the final report and the recommendations from your research study with the GPW management through the Branch: Human Resources.

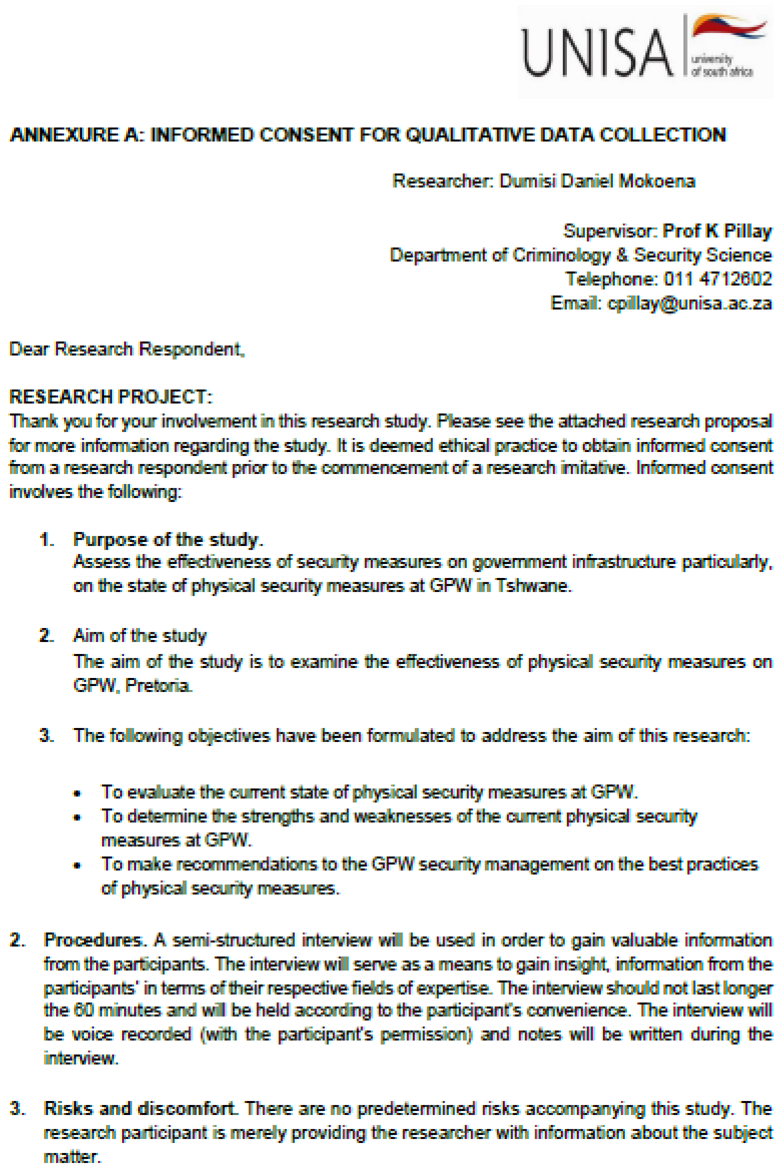
You will also be required to ensure that beside your academic institution, only GPW is the legal recipient of your research report.

We wish you well with your academic endeavours.

Yours Faithfully,

MS. M. M. MODISE
GENERAL MANAGER: HUMAN RESOURCES
DATE: 08 / 07 / 2022

Appendix C: Informed Consent for Qualitative Data Collection



ANNEXURE A: INFORMED CONSENT FOR QUALITATIVE DATA COLLECTION

Researcher: Dumisi Daniel Mokoena

Supervisor: **Prof K Pillay**
Department of Criminology & Security Science
Telephone: 011 4712602
Email: cpillay@unisa.ac.za

Dear Research Respondent,

RESEARCH PROJECT:
Thank you for your involvement in this research study. Please see the attached research proposal for more information regarding the study. It is deemed ethical practice to obtain informed consent from a research respondent prior to the commencement of a research imitative. Informed consent involves the following:

1. **Purpose of the study.**
   Assess the effectiveness of security measures on government infrastructure particularly, on the state of physical security measures at GPW in Tshwane.

2. Aim of the study
   The aim of the study is to examine the effectiveness of physical security measures on GPW, Pretoria.

3. The following objectives have been formulated to address the aim of this research:

   - To evaluate the current state of physical security measures at GPW.
   - To determine the strengths and weaknesses of the current physical security measures at GPW.
   - To make recommendations to the GPW security management on the best practices of physical security measures.

2. **Procedures.** A semi-structured interview will be used in order to gain valuable information from the participants. The interview will serve as a means to gain insight, information from the participants' in terms of their respective fields of expertise. The interview should not last longer the 60 minutes and will be held according to the participant's convenience. The interview will be voice recorded (with the participant's permission) and notes will be written during the interview.

3. **Risks and discomfort.** There are no predetermined risks accompanying this study. The research participant is merely providing the researcher with information about the subject matter.

4. **Benefits.** There are no perceptible benefits or incentives available for the respondents of this study. However, it can be proposed that the research participant will benefit in some way through the process of knowledge production. If the researcher receives permission from the respondent, the researcher will publish their names in the final dissertation.

5. **Respondent's rights.** Respondents are at liberty to withdraw from the study at any stage of the research provided a courtesy notification of withdrawal is sent to the researcher or during the actual interview as well. No negative repercussions will be enacted on the respondent, since participation is voluntary and all data received from the respondent will be taken as void.

6. **Confidentiality.** All information will be regarded as personal and confidential. The researcher will not disclose any respondents' names or contact details unless permission to do so is first obtained.

7. **Data storage and dissemination of findings.** The information received from any respondent/interviewee will be stored (password protected) by the researcher. The findings of the research will be documented in the form of an academic dissertation.

8. **Ethical considerations.** The study was ethically constructed and approved by UNISA's Ethical Committee.

9. **Questions and concerns.** The researcher welcomes any questions or concerns regarding the research study.

10. **Storage and data retention**
    Data that will be collected and stored in secure and password protected computer. The data will be retained for a minimum of 10 years after which it will be destructed in order to avoid violation of POPIA act on private information.

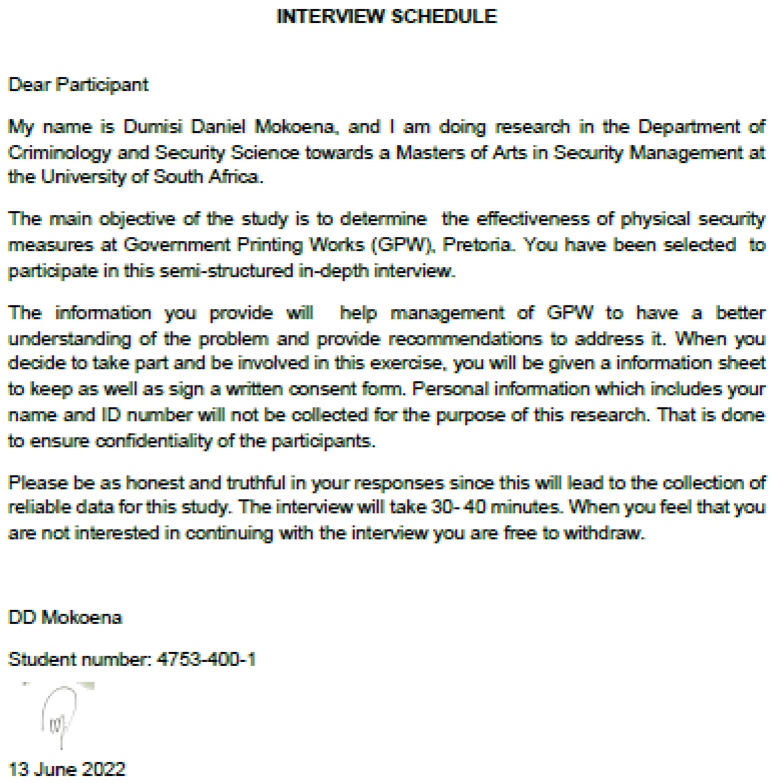
11. **Dissemination of research products.**
    The research will be available for your readings in the University of South Africa Institutional repository.

If in agreement with the above to voluntarily participate in the abovementioned research study, please provide your initials and surname below:

I understand my rights as a research respondent/interviewee and voluntarily give my consent to participate.	
Research respondent: Bila Kurhula	**Date:** 25/07/2022
Signed:	
Researcher: UNISA Student No. 4753-400-1	**Date:**
Signed:	

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix D: Interview Schedule



INTERVIEW SCHEDULE

Dear Participant

My name is Dumisi Daniel Mokoena, and I am doing research in the Department of Criminology and Security Science towards a Masters of Arts in Security Management at the University of South Africa.

The main objective of the study is to determine the effectiveness of physical security measures at Government Printing Works (GPW), Pretoria. You have been selected to participate in this semi-structured in-depth interview.

The information you provide will help management of GPW to have a better understanding of the problem and provide recommendations to address it. When you decide to take part and be involved in this exercise, you will be given a information sheet to keep as well as sign a written consent form. Personal information which includes your name and ID number will not be collected for the purpose of this research. That is done to ensure confidentiality of the participants.

Please be as honest and truthful in your responses since this will lead to the collection of reliable data for this study. The interview will take 30- 40 minutes. When you feel that you are not interested in continuing with the interview you are free to withdraw.

DD Mokoena

Student number: 4753-400-1

13 June 2022

Section A: General demographic information.

1. Gender

Male	
Female	

2. Age group

Less than 25 years	
25-30 years	
31-35 years	
36-40 years	
More than 40 years	

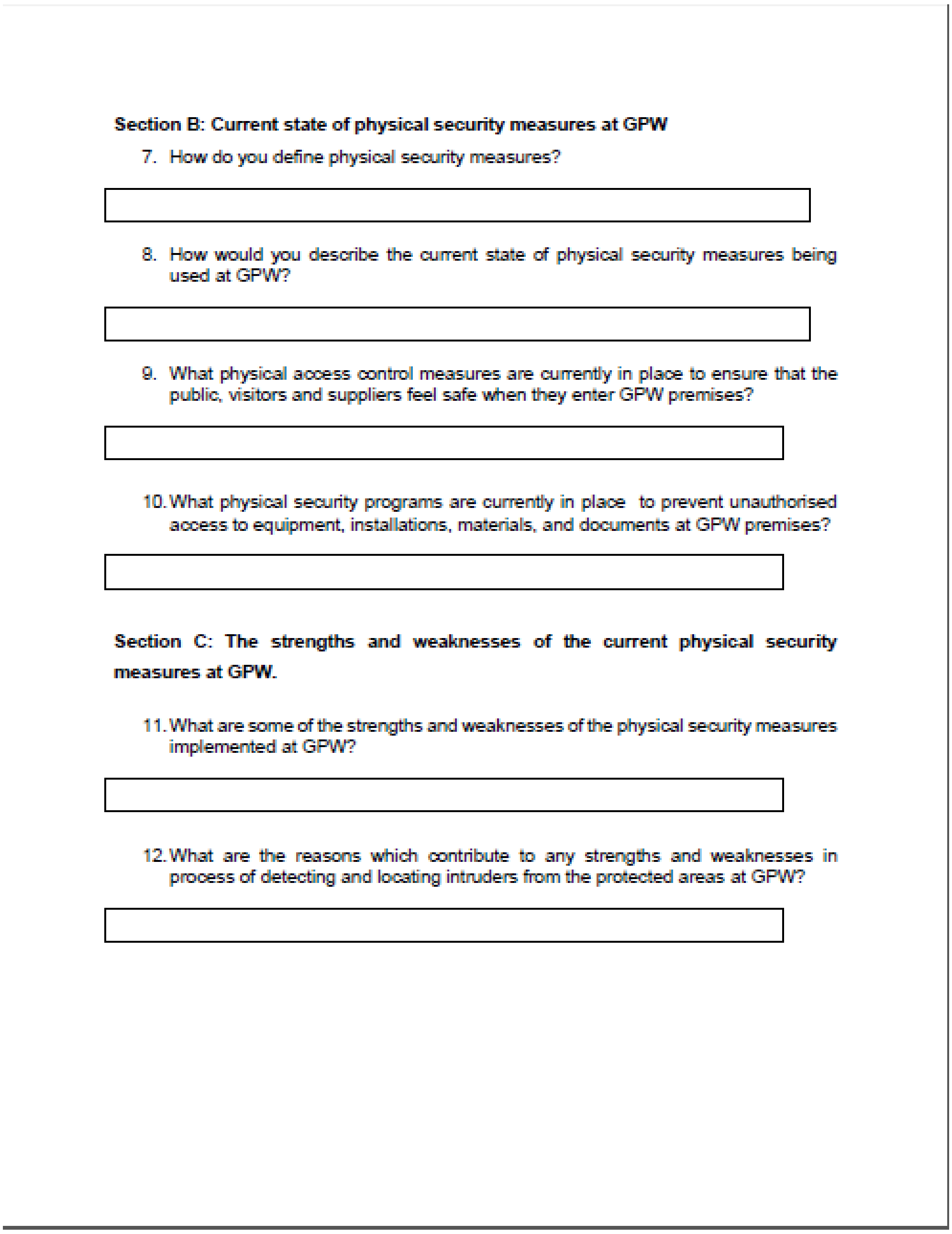
3. What is your highestacademic qualification?

4. How long have you been working at the Government Printing Works as a security personnel ?

5. What is your current role in the security department of GPW?

6. What grade are you on PSIRA

Grade E	Grade D	Grade C	Grade B	Grade A



Section B: Current state of physical security measures at GPW

7. How do you define physical security measures?

8. How would you describe the current state of physical security measures being used at GPW?

9. What physical access control measures are currently in place to ensure that the public, visitors and suppliers feel safe when they enter GPW premises?

10. What physical security programs are currently in place to prevent unauthorised access to equipment, installations, materials, and documents at GPW premises?

Section C: The strengths and weaknesses of the current physical security measures at GPW.

11. What are some of the strengths and weaknesses of the physical security measures implemented at GPW?

12. What are the reasons which contribute to any strengths and weaknesses in process of detecting and locating intruders from the protected areas at GPW?

TRAINING:

13. What types of security training does GPW offer staff who are responsible for implementing physical access control measures at the orgainsation?

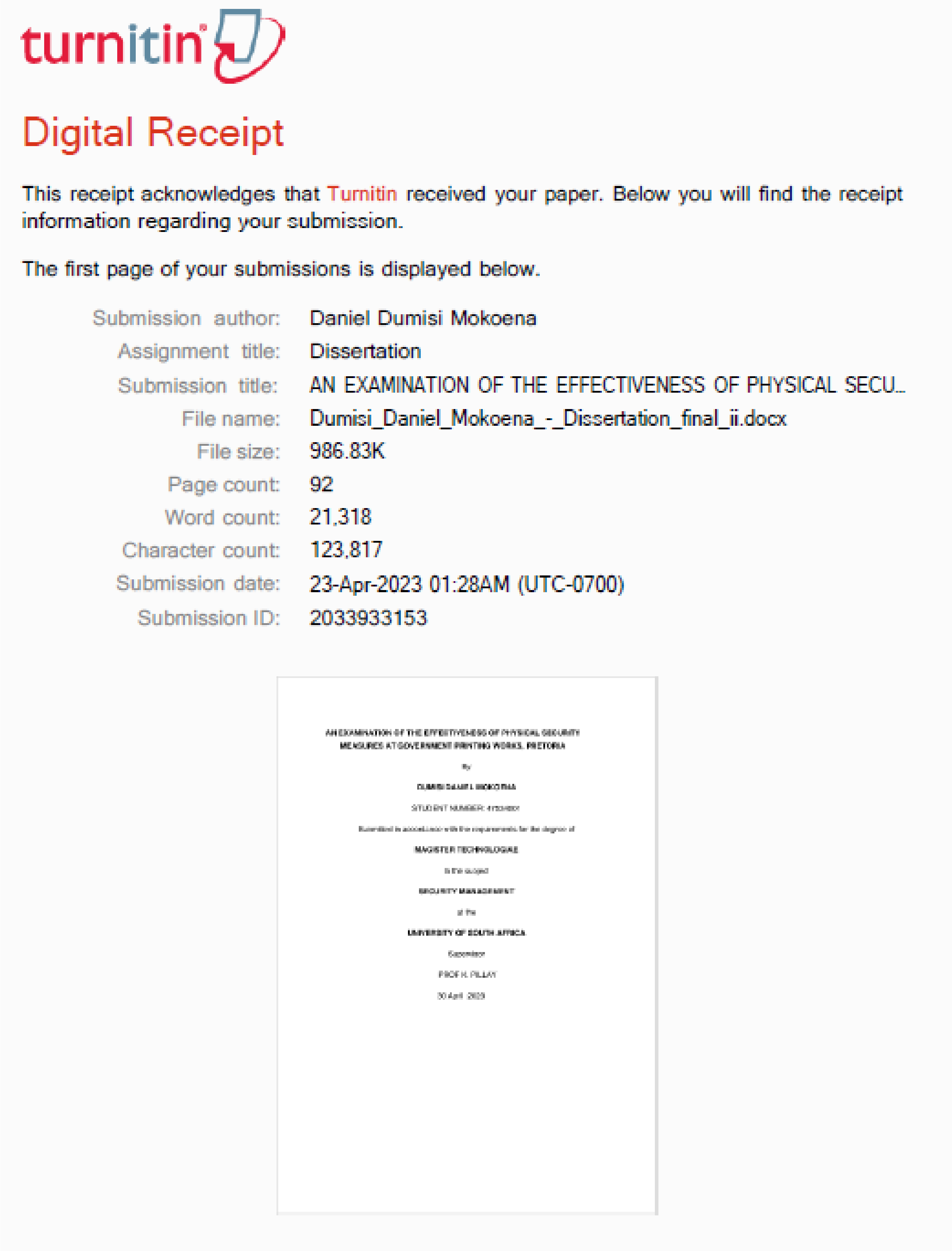
14. How effective is the training on the implementation of physical access control measures at GPW?

Section C: Recommendations to the GPW security management on the best practices of physical security measures.

15. What additional measures would you think can be implemented at GPW, assuming that the security measures are not adequate for the process of detecting and locating intruders from the protected areas?

Thank you for your participation.

Appendix E: Turnitin Digital Report



turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Daniel Dumisi Mokoena
Assignment title:	Dissertation
Submission title:	AN EXAMINATION OF THE EFFECTIVENESS OF PHYSICAL SECU...
File name:	Dumisi_Daniel_Mokoena_-_Dissertation_final_ii.docx
File size:	986.83K
Page count:	92
Word count:	21,318
Character count:	123,817
Submission date:	23-Apr-2023 01:28AM (UTC-0700)
Submission ID:	2033933153

AN EXAMINATION OF THE EFFECTIVENESS OF PHYSICAL SECURITY MEASURES AT GOVERNMENT PRINTING WORKS, PRETORIA

By

DUMISI DANIEL MOKOENA

STUDENT NUMBER: [illegible]

Submitted in accordance with the requirements for the degree of

MAGISTER TECHNOLOGIAE

in the subject

SECURITY MANAGEMENT

at the

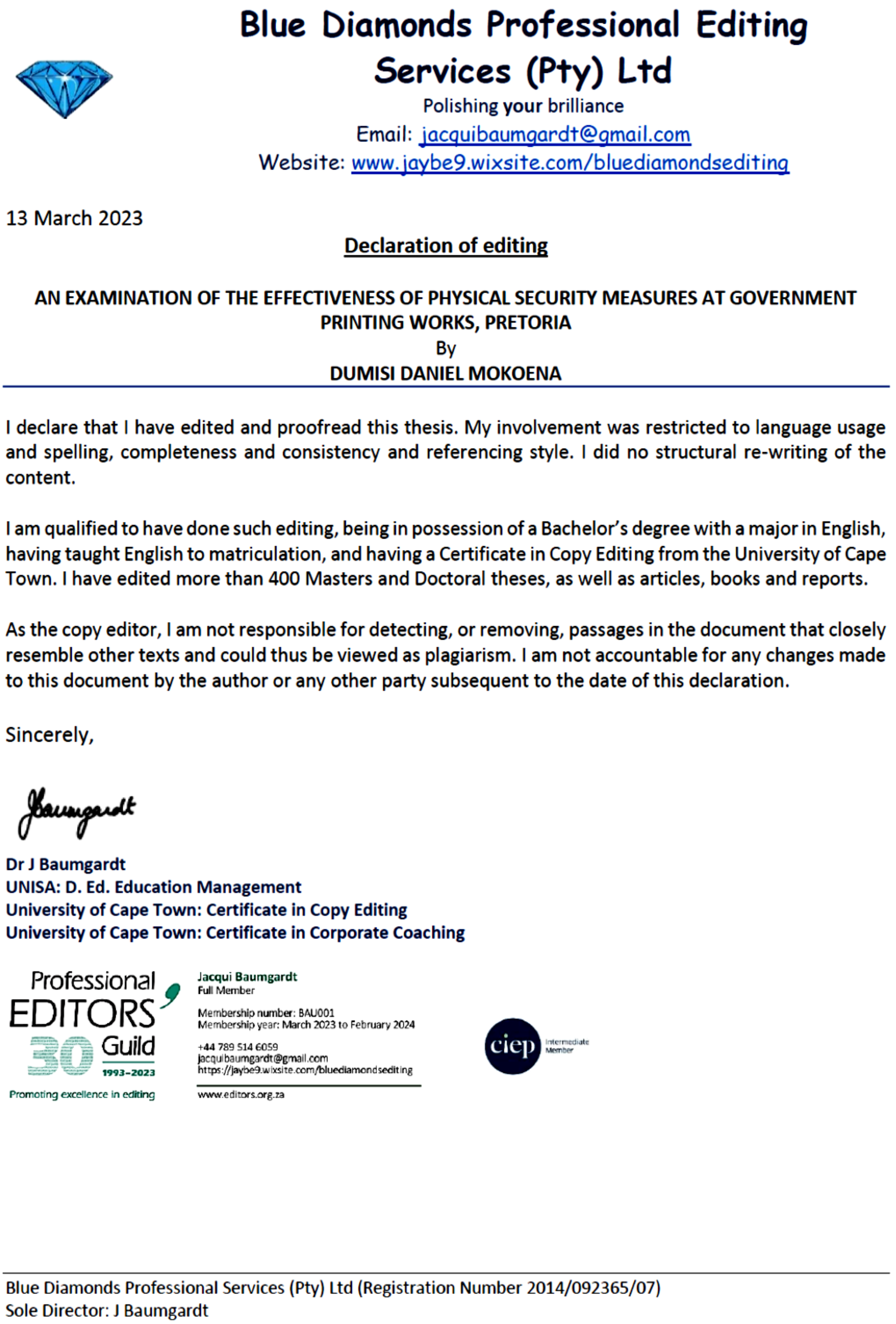
UNIVERSITY OF SOUTH AFRICA

Supervisor

PROF K. PILLAY

30 April 2023

Appendix F: Editor’s Report



Blue Diamonds Professional Editing Services (Pty) Ltd

Polishing your brilliance
Email: jacquibaumgardt@gmail.com
Website: www.jaybe9.wixsite.com/bluediamondsediting

13 March 2023

Declaration of editing

AN EXAMINATION OF THE EFFECTIVENESS OF PHYSICAL SECURITY MEASURES AT GOVERNMENT PRINTING WORKS, PRETORIA
By
DUMISI DANIEL MOKOENA

I declare that I have edited and proofread this thesis. My involvement was restricted to language usage and spelling, completeness and consistency and referencing style. I did no structural re-writing of the content.

I am qualified to have done such editing, being in possession of a Bachelor’s degree with a major in English, having taught English to matriculation, and having a Certificate in Copy Editing from the University of Cape Town. I have edited more than 400 Masters and Doctoral theses, as well as articles, books and reports.

As the copy editor, I am not responsible for detecting, or removing, passages in the document that closely resemble other texts and could thus be viewed as plagiarism. I am not accountable for any changes made to this document by the author or any other party subsequent to the date of this declaration.

Sincerely,

JBaumgardt

Dr J Baumgardt
UNISA: D. Ed. Education Management
University of Cape Town: Certificate in Copy Editing
University of Cape Town: Certificate in Corporate Coaching

Professional EDITORS Guild
30
1993–2023
Promoting excellence in editing

Jacqui Baumgardt
Full Member

Membership number: BAU001
Membership year: March 2023 to February 2024

+44 789 514 6059
jacquibaumgardt@gmail.com
https://jaybe9.wixsite.com/bluediamondsediting

www.editors.org.za

ciep Intermediate Member

Blue Diamonds Professional Services (Pty) Ltd (Registration Number 2014/092365/07)
Sole Director: J Baumgardt