Institute of Petroleum Studies - Kampala

EMPLOYEE PHYSICAL SECURITY TRAINING AND INCIDENT RESPONSE EFFICIENCY: A CASE STUDY OF CNOOC, HOIMA DISTRICT, UGANDA

AGABA GODWIN

M23M03/004

A DISSERTATION

SUBMITTED TO THE FACULTY OF ENERGY AND MANAGEMENT STUDIES IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF A DEGREE OF MASTER OF BUSINESS ADMINISTRATION IN OIL AND GAS OF INSTITUTE OF PETROLEUM STUDIES KAMPALA.

MARCH, 2025

Declaration

I, Agaba Godwin, hereby declare that, this is my original work and has not been presented to any University or Institutions of higher learning for any Academic Award.

Signed:…….. Date: 25th March 2025

Approval

This is to certify that, this dissertation entitled "**EMPLOYEE PHYSICAL SECURITY TRAINING AND INCIDENT RESPONSE EFFICIENCY: A CASE STUDY OF CNOOC, HOIMA DISTRICT, UGANDA**" has been done under my supervision and now it is ready for submission.

Signature: ……..

Supervisor's Name: Prof. Bruno Lule YAWE

Date: 25th March 2025.

Dedication

I dedicate this research to my family to appreciate them for giving me moral support throughout this programme.

Acknowledgement

Throughout this research, I benefited from advice and guidance from a number of individuals without whom, it would have been difficult for this study to be successful. I shall forever be indebted to them.

To begin with, special thanks go to my supervisor for his professional supervision from the commencement of this research until its conclusion.

To the staff of CNOOC Hoima district and other leaders, thank you so much for your time and timely feedback to the questions that were asked.

I am also indebted to my course mates with whom we had fruitful discussions in and outside classroom. I am forever indebted.

God Bless you all.

Table of Contents

List of Tables and Figures

Figures

List of Abbreviations

BSEE	Bureau of Safety and Environmental Enforcement
CNOOC	China National Offshore Oil Corporation
EAC	East African Community
IOG	International Association of Oil & Gas Producers (IOG
NIMASA	Nigerian Maritime Administration and Safety Agency
NOPSEMA	National Offshore Petroleum Safety and Environmental Management Authority
PEOU	Perceived Ease of Use
PSA	Petroleum Safety Authority Norway
PU	Perceived Usefulness SEMs
SEMSs	Safety and Environmental Management Systems
SPSS	Statistical Package for Social Scientists
TAM	Technology Acceptance Model

Abstract

The general objective of the study was to evaluate the influence of employee physical security training on the efficiency of incident response in Ugandan oil and gas companies, specifically focusing on CNOOC in Hoima District. The study was guided by the following objectives, to assess the impact of employee physical security training on the effectiveness of access control measures in incident response at CNOOC, Hoima District, to evaluate how employee physical security training influences the implementation and adherence to facility security protocols during incident response at CNOOC, Hoima District, and to evaluate the role of security training in improving access control during incidents at CNOOC. Cross-sectional survey design was used. The study predominantly employed a quantitative approach but also used a qualitative approach. The study population consisted of 200 participants. A sample size of 147 respondents was selected using simple and purposive sampling techniques. Quantitative data analysis mainly consisted of descriptive statistics (percentages, frequencies). Content analysis was used to analyse qualitative data. The study findings showed that employee physical security training significantly enhances the ability of personnel to implement access control measures effectively during incidents. Clear guidelines and relevant protocols foster greater engagement and adaptability among employees. Thorough training increases employees' confidence in following security protocols, leading to higher adherence during incidents. However, challenges remain, particularly in communication and coordination, which can hinder effective incident responses. Training enhances coordination and teamwork among security personnel, leading to improved incident management. Regular collaborative exercises reinforce trust and preparedness, while employee feedback can help refine current coordination processes. The findings underscore the vital importance of employee physical security training in strengthening incident response capabilities at CNOOC. Enhanced training not only improves adherence to access control measures and security protocols but also fosters better coordination among security personnel, ultimately contributing to a more resilient security framework. It was recommended that CNOOC should prioritize the development and implementation of comprehensive, ongoing employee physical security training programs that include regular feedback mechanisms and collaborative exercises. This approach will address communication gaps, reinforce protocols, and ensure that employees remain engaged and well-prepared to effectively manage security incidents.

CHAPTER ONE

INTRODUCTION

1.1 Background to the study

Employee physical security training is a structured process aimed at equipping staff with the necessary skills and knowledge to recognize and address potential security threats within their workplaces. This training involves educating employees on various risks such as theft, unauthorized access, and workplace violence, alongside essential emergency response protocols and proper use of security systems (Nkosi & Okafor, 2022). By integrating both theoretical frameworks and practical applications, organizations can enhance employees' ability to respond effectively to security incidents, thereby fostering a safer work environment tailored to specific local contexts and vulnerabilities (Yusuf, 2020). The training methods may include practical workshops, simulations, and e-learning modules designed to engage employees with diverse learning styles (Chikezie, 2021).

The effectiveness of physical security training is crucial for creating a secure workplace atmosphere, as it empowers employees to take prompt and appropriate actions during security incidents. Research indicates that comprehensive training programs can lead to reduced incident occurrence and improved response times, contributing significantly to the overall safety of the workplace (Banda & Mwale, 2023). Additionally, ongoing assessments and feedback mechanisms are vital for evaluating the efficacy of these training initiatives, ensuring that employees remain aware of emerging security challenges and best practices (Suleiman, 2021). By emphasizing employee physical security training through the lens of African scholarship, organizations can implement robust strategies that enhance employee preparedness and contribute substantially to workplace safety and security (Adebayo & Farah, 2020).

The significance of employee physical security training in enhancing incident response efficiency has garnered considerable attention globally, particularly within the oil and gas sector. The ongoing evolution of security threats necessitates comprehensive training programs designed to equip personnel with the necessary skills to mitigate risks effectively. This need is underscored by a 35% increase in global security incidents in the oil and gas industry from 2010 to 2020, as reported by the International Association of Oil & Gas Producers (IOGP) in 2021, highlighting the urgency for enhanced security measures in this high-stakes environment.

Prominent incidents, such as the Deepwater Horizon oil spill in 2010, illustrate critical deficiencies in incident response frameworks that could have been addressed through improved training, particularly in access control, facility security protocols, and emergency response plans. In the U.S., regulations mandated by the Bureau of Safety and Environmental Enforcement (BSEE) led to the implementation of the Safety and Environmental Management Systems (SEMS), resulting in a 23% reduction in incident response times and a 17% boost in incident resolution efficiency from 2013 to 2020 (BSEE, 2021).

Globally, countries like Norway have witnessed the benefits of rigorous security training, reporting a 15% decrease in security-related incidents and a 20% increase in successful incident resolutions from 2015 to 2020, as stated by the Petroleum Safety Authority Norway (PSA). Australia has also prioritized rigorous training, leading to an 18% reduction in significant incidents and a 22% improvement in response times between 2014 and 2020, highlighting the essential role of tailored security training programs (NOPSEMA, 2021).

Focusing on Africa, particularly countries like Nigeria and Angola, the region faces unique security challenges such as oil theft and militant attacks on infrastructure. A study by Okon and Adebayo (2019) emphasizes that comprehensive physical security training significantly improves response times in these contexts. For instance, Nigeria's establishment of the Nigerian Maritime Administration and Safety Agency (NIMASA) has enhanced maritime security through targeted training, allowing for more effective management of security incidents (Ajayi & Omotayo, 2021).

In East Africa, Uganda's burgeoning oil sector, particularly in the Albertine Graben area, has introduced both opportunities and security challenges. The country has faced concerns related to land disputes, theft, and the threat of terrorism. Regional collaboration and targeted physical security training have been pivotal in addressing such threats. Reports indicate that the East African Community (EAC) has initiated training programs aimed at improving safety and security in oil and gas operations (Mugisha, 2019).

The China National Offshore Oil Corporation (CNOOC) operates in Hoima District, Uganda, where significant investments in infrastructure and training have been made. Local studies by Nakabugo (2022) and Tumwine (2021) highlight substantial gaps in security training frameworks. Instances of unauthorized access to restricted areas, theft, and delays in incident response times have underscored the need for improved training protocols. Notably, while technological advancements are valuable, the capability and readiness of the workforce

remain critical for effective response to security incidents. CNOOC has faced multiple security challenges that necessitate a robust training regime, moving beyond mere compliance to foster a culture of proactive security awareness among employees.

This study aimed to assess the impact of employee physical security training on incident response efficiency: a case study of CNOOC, Hoima district, Ugandan. By focusing on local security challenges and drawing insights from international practices, the objective is to identify key areas for enhancing training programs to bolster overall incident response capabilities, thereby promoting the safety and stability of Uganda's rapidly developing oil and gas sector. Emphasizing the local context will inform tailored strategies that address Uganda's unique security landscape, highlighting the importance of developing a workforce that is not only well-trained but also adaptive to emerging threats in the industry.

1.2 Statement of the problem

The oil and gas sector in Uganda, particularly at CNOOC in Hoima District, faces significant challenges concerning the preparedness of its workforce to effectively respond to security incidents. Past empirical studies, such as Banda (2020) and Chukwu (2019), have highlighted the importance of effective security training in enhancing employee readiness in high-risk environments. However, despite the investment from both the government and CNOOC into various security training programs, critical gaps persist that undermine the effectiveness of these initiatives and the overall security framework.

Firstly, current training approaches often rely heavily on theoretical knowledge without integrating contemporary risk scenarios. This outdated methodology has been noted by Munyua and Muturi (2019), who found that theoretical training disconnected from practical application leads to a workforce that may struggle to act decisively in real incidents. The reliance on traditional methods limits employees' practical understanding of security threats, which becomes particularly problematic when unexpected situations arise. Secondly, many existing programs lack comprehensive scenario-based training that reflects the specific threats faced within the oil and gas sector. Alemayehu (2020) emphasized the necessity for practical exercises to prepare employees for real-world challenges; without opportunities to engage in realistic drills and simulations of security incidents, employees may find themselves ill-equipped to respond effectively during crises. This not only leads to potential delays and confusion but can also endanger the safety of personnel and assets.

Furthermore, the training curriculum is not regularly updated to keep pace with rapidly evolving security threats. Research by Ngugi and Mwangi (2020) demonstrates that organizations failing to adapt their training accordingly often leave their workforce ill-prepared to manage modern risks effectively. Employees may become trained on outdated protocols that do not address current vulnerabilities, exacerbating the problem of preparedness.

Observations by Nakabugo (2022) reveal specific issues at CNOOC, including unauthorized access to restricted areas and inadequate perimeter security measures. These findings align with the conclusions of Tusiime (2021), who articulated that inadequate emphasis on access control procedures and incident response protocols leads to slow response times and an increased likelihood of security breaches. The lack of integrated, continuous security training that focuses on these critical areas represents a significant gap in the current framework at CNOOC. Despite these identified issues, there exists a knowledge gap concerning the effectiveness of tailored, scenario-based training initiatives that integrate technological advancements as advocated by Mungai and Kamau (2018) and Tusiime (2021). This study, therefore, aimed to investigate the existing training programs at CNOOC to identify specific shortcomings and propose a robust model for enhancing employee preparedness against security incidents, thereby addressing the critical gaps identified in previous empirical studies.

1.3 Purpose of the study

The study sought to assess the impact of employee physical security training on incident response efficiency

1.4 Specific Research Objectives

The study was guided by three specific objectives, namely;

1. To assess the impact of employee physical security training on the effectiveness of access control measures in incident response at CNOOC, Hoima District.
2. To evaluate how employee physical security training influences, the implementation and adherence to facility security protocols during incident response at CNOOC, Hoima District.
3. To evaluate the role of security training in improving access control during incidents at CNOOC

1.5 Research questions

1. How does employee physical security training impact the effectiveness of access control measures in incident response at CNOOC, Hoima District?
2. What influence does employee physical security training have on the implementation and adherence to facility security protocols during incident response at CNOOC, Hoima District?
3. What is the role of security training in improving access control during incidents at CNOOC?

1.6 Scope of the study

This study explored the influence of employee physical security training on incident response efficiency in Ugandan oil and gas companies. It focused on assessing the impact of employee physical security training on the effectiveness of access control measures in incident response at CNOOC, Hoima District, evaluate how employee physical security training influences the implementation and adherence to facility security protocols during incident response at CNOOC, Hoima District, and to evaluate the role of security training in improving access control during incidents at CNOOC

This study covered the period from 2017 to the present. This timeframe was selected due to several practical reasons, including significant technological advancements in security technology and methodologies over recent years, which are pertinent to the study. Additionally, updates to industry regulations and standards in Uganda have influenced how companies approach security and incident response. The increased threat landscape, marked by a rise in cyber threats and security incidents, provides a rich dataset for analysis within this period.

The geographical focus of the study was Hoima, located in south-western Uganda. Hoima is a major hub for the oil and gas industry in Uganda, hosting several key facilities and infrastructure projects, making it a highly relevant location for the study. The concentration of oil and gas companies in this area provides an ideal environment to analyze the implementation and effectiveness of security training programs and incident response mechanisms. Moreover, the accessibility of multiple industry players in a relatively concentrated area facilitates data collection and stakeholder engagement. By focusing on Hoima, the study aimed to offer insights directly applicable to the region's oil and gas sector, with potential lessons for other areas with similar industry characteristics.

1.7 Justification of the study

The justification for this study on employee physical security training and its impact on incident response efficiency in Ugandan oil and gas companies is multi-faceted and grounded in both local context and empirical evidence. Firstly, the oil and gas industry in Uganda serves as a crucial contributor to the national economy, underscoring the necessity for robust security measures to safeguard this sector. The National Oil and Gas Policy for Uganda (2018) emphasizes the importance of comprehensive security frameworks, including employee physical security training, to protect the industry's infrastructure and operations from potential threats (Ministry of Energy and Mineral Development, 2018). Given the substantial foreign investments and sensitive nature of oil production and distribution, any lapses in security can have far-reaching economic implications.

Recent incidents in Uganda's oil fields have illustrated the urgent need for enhanced security training measures. For example, in early 2022, unauthorized individuals breached a sensitive area at the Tilenga oil exploration site, resulting in a delay in operations and raising concerns about potential sabotage (local news sources). Such incidents not only disrupt operations but also pose significant risks to the local environment and community safety. These challenges highlight glaring gaps in the current security protocols that could potentially be mitigated through effective employee training programs focused on physical security.

Moreover, local research by Nakalema (2020) on "The Role of Security Management in Enhancing Operational Efficiency in Uganda's Oil and Gas Sector" underscores that well-trained employees are integral to effective security management. Nakalema's findings reveal that employees with robust training are more adept at implementing critical security measures such as authentication methods, authorization levels, physical access control, and access monitoring. These capabilities minimize potential risks and prevent operational disruptions, as demonstrated by the case of a successful intervention in August 2021, where prompt action from trained employees thwarted a potential security breach at a gas storage facility.

Additionally, research conducted by Muhwezi and Kamugisha (2019) on "Security Preparedness in Uganda's Oil and Gas Industry" emphasizes the evolving threat landscape and the pressing need for ongoing physical security training. The authors argue that regular updates to training programs - which include perimeter security, internal security measures, employee awareness initiatives, and technology integration—are essential. These enhancements equip employees with the necessary skills to confront emerging security

challenges effectively. Empirical examples from neighbouring East African nations, such as Kenya, which has faced similar security threats in its oil sectors, further support the necessity of a continuous training regimen to address security vulnerabilities effectively.

The importance of post-incident analysis and continuous improvement in incident response is mirrored in the recommendations from the Petroleum Authority of Uganda (PAU) in their 2021 annual report. The PAU advocates for systematic training and evaluation processes in essential areas, such as incident identification, response coordination, evacuation procedures, and post-incident review. These evaluation processes are crucial for enhancing the overall security posture of the oil and gas sector.

1.9 Significance of the study

The significance of this study on employee physical security training and its influence on incident response efficiency in Ugandan oil and gas companies is broad, affecting various stakeholders in the industry.

Government and Regulatory Bodies: For government agencies and regulatory bodies, such as the Ministry of Energy and Mineral Development and the Petroleum Authority of Uganda (PAU), the study provides crucial insights into the effectiveness of current security training programs. It highlights areas where policies can be strengthened to ensure that oil and gas companies comply with national security standards. Improved security practices can lead to enhanced national security and protect critical infrastructure, which is vital for the country's economic stability and growth.

Oil and Gas Companies: For oil and gas companies operating in Uganda, the study emphasizes the importance of investing in comprehensive employee security training programs. By demonstrating the link between effective training and improved incident response efficiency, companies can justify the allocation of resources towards these programs. Enhanced security measures can reduce the risk of operational disruptions, financial losses, and damage to company reputation. Additionally, it can lead to better preparedness and quicker recovery from security incidents, ensuring smoother operations.

Employees: Employees in the oil and gas sector stand to benefit significantly from improved security training. The study underscores the value of being well-prepared to handle security threats, which can enhance employees' confidence and ability to respond effectively to incidents. Well-trained employees are better protected from potential harm and can contribute

more effectively to the overall security and resilience of their organization. This can also lead to greater job satisfaction and professional growth.

Investors and Stakeholders: Investors and other stakeholders, including shareholders and partners, will find the study's findings valuable for assessing the security risk management practices of oil and gas companies. Understanding the correlation between employee training and incident response efficiency can inform investment decisions and foster confidence in the company's commitment to safeguarding its assets. Improved security practices can enhance the company's stability and profitability, making it a more attractive investment.

Local Communities: Local communities in regions like Hoima, where oil and gas operations are concentrated, will benefit from the enhanced security measures resulting from effective training programs. Reduced risk of security incidents can lead to fewer disruptions in local economic activities and greater community safety. Moreover, the study can encourage corporate social responsibility initiatives focused on community awareness and preparedness for potential security threats related to oil and gas operations.

Academic and Research Institutions: For academic and research institutions, the study contributes to the body of knowledge on security management in the oil and gas sector. It provides a foundation for further research on best practices in employee training and incident response. Additionally, it offers data and insights that can be used for developing curricula and training programs aimed at improving security practices in the industry.

1.10 Theoretical framework

The study was guided by Training Transfer Theory (TTT) which examines the process through which employees apply knowledge and skills learned in training to their work environments. It aims to identify the factors that influence the transfer of learning, ensuring that training results in improved job performance and effectiveness in specific tasks or behaviors.

Training Transfer Theory has been influenced by various researchers in the field of adult learning and organizational psychology, but it does not have a single founding figure or year of origin. However, a significant foundational work is attributed to Baldwin and Ford, who published "Transfer of Training: A Review and Directions for Future Research" in 1988, which laid the groundwork for understanding the principles of training transfer.

The assumptions underlying Training Transfer Theory include the belief that training is not an isolated event; rather, it involves a dynamic interplay between the training environment, the work environment, and individual characteristics. Another key assumption is that the effectiveness of training depends on the extent to which employees perceive the training as relevant, acquire the skills intended, and receive on-going support to apply what they have learned in their work settings. Additionally, it is assumed that organizational culture and context significantly influence the transfer process.

The applicability of Training Transfer Theory to the study on the effect of employee physical security training on incident response efficiency in Ugandan oil and gas companies is significant. The theory underscores the importance of training relevance, emphasizing that security training must align with the specific threats and scenarios faced in the Ugandan context to enhance employee engagement and retention. Furthermore, it highlights the critical role of a supportive work environment, whereby managerial encouragement and resources help facilitate the application of learned skills in real-world situations. Individual readiness, including employees' confidence and motivation to apply training, also plays a crucial role in effective transfer. By examining these factors, the study can examined how well-implemented training not only improves employees' preparedness for security incidents but also enhances overall incident response efficiency, ultimately contributing to safer operational environments in the oil and gas sector.

1.11 Conceptual Framework

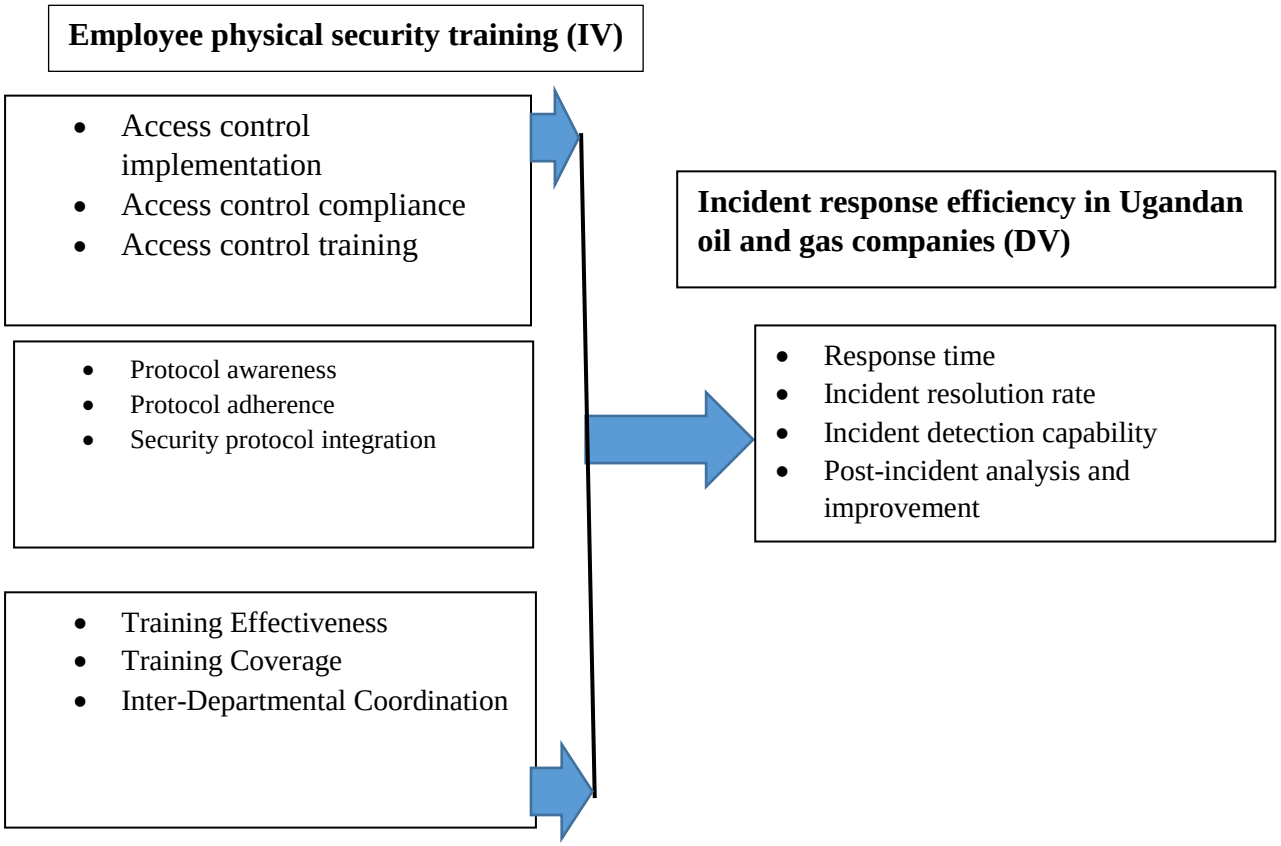

Fig 1.1: Conceptual framework showing the effect of employee physical security training (IV) on incident response efficiency in Ugandan oil and gas companies (DV). *Source:* Davis (1989) a*nd modified by the Researcher*

From Fig 1.1, it was assumed that, the effectiveness of employee physical security training significantly impacts incident response efficiency, which is crucial for maintaining security in the oil and gas sector. The implementation and compliance with access control procedures - such as the use of badges and biometric systems - enhance incident detection capability and reduce response times. When employees are well-trained in access control, the speed and effectiveness of security breach responses improve, leading to quicker incident resolution and more effective post-incident analysis. Similarly, facility security protocols - when well understood and consistently adhered to - prepare employees to handle emergencies more efficiently, integrating various security measures to bolster overall security management. Comprehensive training programs that cover both access control and facility protocols, coupled with frequent and effective training sessions, facilitate better inter-departmental coordination, leading to enhanced incident response efficiency. This integrated approach

ensures that security protocols are not only implemented but continuously reinforced, thereby improving response times, resolution rates, and the capability for effective incident detection and post-incident improvements.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

The study sought to reach the following specific research objectives: (i) To assess the impact of employee physical security training on the effectiveness of access control measures in incident response at CNOOC, Hoima District; (ii) To evaluate how employee physical security training influences, the implementation and adherence to facility security protocols during incident response at CNOOC, Hoima District; and (iii) To evaluate the role of security training in improving access control during incidents at CNOOC.

2.1 Theoretical literature review

The study is guided by Training Transfer Theory (TTT), which examines the process through which employees apply the knowledge and skills acquired during training to their actual work environments. This theory aims to identify the factors that influence the transfer of learning, ensuring that training results in improved job performance and effectiveness in specific tasks or behaviors. TTT emphasizes that effective training is not merely about content delivery but also about how well employees can translate learned skills into practical application in their jobs (Baldwin & Ford, 1988).

A foundational work in Training Transfer Theory is attributed to Baldwin and Ford (1988), who published "Transfer of Training: A Review and Directions for Future Research." Their study laid the groundwork for understanding the principles of training transfer and identified three critical factors influencing this process: the characteristics of the training program, the characteristics of trainees, and the work environment in which the skills must be implemented.

Effective physical security training programs should include relatable, practical, and job-relevant content that resonates with employees. The training methodology should employ varied instructional strategies that cater to different learning styles and preferences. Research indicates that well-structured training increases the likelihood that employees will perceive the value of their training, ultimately promoting better retention and application of the skills learned (Baldwin & Ford, 1988). This aspect underscores the importance of designing programs that are engaging and directly applicable to the unique challenges faced in the workplace.

Individual attributes such as motivation, prior knowledge, and self-efficacy significantly affect employees' ability to transfer learned skills to their job contexts (Burke & Hutchins, 2007). Understanding these characteristics allows organizations to tailor training initiatives to meet employees' distinct needs, thereby enhancing overall engagement and commitment to adopting security protocols. For instance, motivated employees who believe they can successfully implement what they learned are more likely to engage actively in security training and apply their knowledge effectively.

The broader organizational context plays a pivotal role in the transfer of training. Supportive managerial structures, positive peer influence, and a culture that emphasizes the importance of security training can facilitate a smoother transition from learning to application. Research shows that creating an environment that encourages open communication and feedback can further reinforce the relevance of training and its integration into daily practices (Saks & Belcourt, 2006). For example, when management actively supports training initiatives and provides reinforcement, employees are more likely to see the significance of what they learned and apply it in their roles.

Training Transfer Theory (TTT) is a vital framework in workforce development that explores the efficacy of training programs and their impact on employee performance. Central to TTT is the understanding that mere delivery of content does not guarantee that employees will effectively apply acquired skills in their work environments. Baldwin and Ford (1988) identify three critical factors influencing the transfer of training: the characteristics of the training program, the attributes of the trainees, and the contextual features of the work environment. Consequently, the design of training must go beyond the curricular content to consider how trainees engage with the material and how supportive the workplace culture is regarding skill application. Effective training programs should, therefore, incorporate elements that foster engagement and situate learning within relevant job contexts, as this encourages employees to translate learning into practical actions (Baldwin & Ford, 1988).

Moreover, TTT emphasizes the necessity for on-going support and reinforcement to enhance the transfer of learning post-training. Effective follow-up strategies, such as coaching, mentoring, and access to relevant resources, can significantly impact the retention and practical application of the skills learned (Baldwin & Ford, 1988). Additionally, aligning training objectives with organizational goals is crucial in establishing the relevance of training experiences to employees' daily responsibilities. When employees perceive a clear

connection between their training and their job functions, their motivation to apply new knowledge increases, ultimately fostering sustained behavioral change and improved job performance (Blume et al., 2010). Therefore, a comprehensive understanding and application of TTT are essential for organizations striving to maximize the return on investment in training initiatives, ensuring that the outcomes extend beyond learning to tangible improvements in workplace effectiveness (Baldwin & Ford, 1988; Blume et al., 2010).

2.2 Methodological literature review

Okoth (2021) investigated the effectiveness of various training methodologies on enhancing employees' readiness to respond to security incidents. His study systematically employed a mixed-methods approach, combining quantitative surveys with qualitative interviews to capture a comprehensive view of employee perceptions. However, while his research provided valuable insights into how different training modalities affect employee behavior, it also highlighted a common limitation in the literature: the tendency to overlook longitudinal impacts. This gap suggests that while immediate training outcomes can be measured effectively, understanding how these skills are retained over time is crucial for assessing overall training efficacy.

Similarly, Lindström et al. (2019) conducted a qualitative analysis exploring employees' attitudes toward physical security training within a corporate context. Their research underscored a significant divergence in employee engagement based on the perceived relevance and applicability of the training content. Although their findings provided a thorough exploration of individual motivations, they also revealed the need for more systematic integration of these qualitative insights into broader quantitative frameworks. This synthesis of methodologies points to the value of triangulating data sources to capture a fuller picture of training effectiveness across different organizational settings.

Furthermore, Ahmad et al. (2019) contributed to the discourse by examining the comparative effectiveness of various training formats through experimental design. Their approach not only highlighted differences in the impact of hands-on simulations versus traditional classroom training but also illuminated critical factors such as organizational culture that mediate training outcomes. However, their study fell short of considering employee diversity in the analysis. Recognizing the varied demographics and experiences of employees could enrich the understanding of how training is received and applied in practice, thereby reinforcing the arguments made by other scholars advocating for tailored training approaches.

Ultimately, the synthesis of these arguments reveals the importance of methodological diversity in studying the effectiveness of physical security training. While quantitative studies offer robust data on training outcomes, qualitative insights are essential for understanding the nuances of employee perceptions and experiences. As suggested by Schmidt and Hunter (2019), a rigorous exploration of both immediate and long-term training effects can yield critical insights that inform future interventions and policy-making in organizational training practices, aligning closely with the imperative to enhance incident response readiness in today's security environments.

2.2 Empirical literature review

2.2.1 Impact of employee physical security training on the effectiveness of access control measures

In Japan, Saito (2020) conducted an extensive study examining the impact of comprehensive physical security training on access control measures in corporate environments. His research revealed that companies implementing robust training programs saw significant improvements in employee awareness and adherence to access protocols. However, Saito criticized the overly rigid nature of these training programs, which often did not adapt to the dynamic security landscape faced by organizations. This highlights an important consideration for CNOOC: are their training initiatives agile enough to respond to rapidly evolving threats? The application of flexible training models could bolster security effectiveness in Uganda, offering a strategic advantage in an increasingly complex operational environment.

Similarly, a study by Chen et al. (2019) in the United States underscores the importance of technology integration in physical security training. Their research found that organizations with a high degree of technological proficiency, such as those employing advanced data analytics for threat detection, experienced enhanced effectiveness in access control measures. However, the study also pointed out that many organizations did not sufficiently equip their employees with the necessary training to utilize these technologies effectively. This gap poses a challenge for CNOOC, as the interplay between technology and training is vital to optimizing access control. An exploration of how CNOOC can integrate available technologies into its training programs may reveal avenues for improving security measures, particularly in a resource-constrained environment.

Furthermore, the findings of Robinson and Glover (2021) highlight the significance of a multi-faceted training approach in enhancing physical security measures in corporate America. Their research suggests that organizations that combined traditional training methods with simulations and scenario-based exercises witnessed improved retention of security protocols among employees. Though their emphasis was on internal security threats, the implications for CNOOC's training programs are clear: employing a diverse range of training techniques could lead to higher employee engagement and effectiveness in maintaining access control measures. Exploring the feasibility of incorporating such innovative training approaches could yield beneficial outcomes for CNOOC's security posture in Uganda.

Tusiime (2021) highlights a critical gap in integrating employee training with technological advancements in security measures. His research indicates that organizations in these areas often utilize cutting-edge security technologies, yet they frequently fail to incorporate relevant training programs for employees, which diminishes the overall effectiveness of access control systems. This finding emphasizes a crucial aspect for CNOOC, where the availability of advanced technological resources may be limited. A nuanced inquiry into how employee training can be optimized alongside existing security technologies becomes essential for enhancing access control measures in environments where financial constraints exist.

Banda (2020) explores the essential role of regular training programs in mitigating internal threats within Nigerian oil companies. While he presents compelling evidence of reduced unauthorized access incidents in organizations with comprehensive training, he critiques the limited integration of training with advanced technological tools, such as biometric systems. This observation raises an important question for CNOOC in Uganda: can employee training alone sufficiently guard against unauthorized access in environments with limited technological infrastructure? The specific socio-political context in Uganda requires an investigation into how training might compensate for technological shortcomings while addressing unique local challenges.

Alemayehu (2020) acknowledges that while physical security training enhances access control, a substantial gap exists in continuous professional development. His study found that employees in Ethiopian organizations often lack ongoing training, which leaves them inadequately prepared to address emerging threats. Within CNOOC, which operates in a

rapidly evolving sector, the inadequacy of continuous professional development is particularly concerning. Therefore, analyzing how CNOOC structures its training programs for continuous professional development is crucial, especially regarding industry trends and evolving security threats.

Additionally, Munyua and Muturi (2019) examine the limitations of a uniform training approach in Kenyan organizations, highlighting the failure to tailor security training to the specific needs of different facilities. This observation raises a pertinent gap for CNOOC: Are their training programs sufficiently customized to address environmental risks unique to Ugandan operations? A critical assessment of whether CNOOC employs a flexible training model to mitigate vulnerabilities within their specific security landscape versus adopting a standardized approach could provide insight into the potential effectiveness of their training efforts.

Moreover, taking a cross-national perspective, Mungai and Kamau (2018) criticize the reliance on external training providers in the Kenyan oil sector. They argue that these providers often lack a comprehensive understanding of local security challenges. This criticism can extend to CNOOC, warranting an investigation into whether external training providers are adequately addressing the company's context in Uganda or if there is potential for developing bespoke in-house training programs that resonate with local security concerns. Capitalizing on in-house capabilities might enhance the overall effectiveness of security training initiatives.

Ngugi and Mwangi (2020) advance the dialogue by discussing inter-departmental coordination issues affecting access control measures. Their findings indicate that siloed approaches inhibit effective application, an observation that could be applicable to CNOOC. Examining the dynamics of collaboration among different departments in the implementation of access control measures could reveal systemic organizational challenges, possibly stemming from inadequate training.

Kisakye (2022) emphasizes the critical need for post-training evaluations to assess the effectiveness of security training programs. For organizations like CNOOC, implementing systematic evaluations is vital for continuous improvement in their security posture. Understanding the impact of training on access control measures not only lends itself to better

resource allocation but also helps in identifying and addressing potential weaknesses in security practices.

Nuwagaba (2023) argues for greater integration between training programs and overall security protocols at CNOOC, suggesting that a holistic approach to training could prevent fragmented security practices that might be vulnerable to exploitation. This reinforces the need for an integrative framework that aligns employee training with the organization's comprehensive security strategy, thereby enhancing resilience against potential threats.

2.2.2 Influence of employee physical security training on implementation and adherence to facility security protocols

Employee physical security training has emerged as a critical factor in reinforcing adherence to facility security protocols across various industries. In high-income countries, studies have underscored the direct correlation between well-structured training programs and employee compliance with security measures. For instance, in a comprehensive assessment of U.S. corporations, Smith and Wiggins (2019) found that organizations that prioritized ongoing training not only improved safety outcomes but also fostered a culture of vigilance that permeated all levels of staff. This underscores the potential for similar approaches to enhance security measures within CNOOC, as cultivating a proactive security mindset among employees may correspondingly bolster adherence to established protocols.

Adding to this discourse, Johnson and Franklin (2020) explored the dynamics of training in the European context, advocating for the integration of scenario-based exercises that simulate real-world threats. Their findings revealed that employees who engaged in practical scenarios reported substantially higher confidence levels and adherence to security protocols compared to those only exposed to theoretical frameworks. This highlights a critical aspect for CNOOC: evaluating whether their training curriculum includes practical exercises tailored to the unique challenges of the Ugandan oil sector, which could significantly improve employee preparedness and compliance.

A study by Mwangi and Ngugi (2019) in Kenya illustrated the importance of contextualizing security training to local operational challenges. Their research emphasized that generic training content often fails to address specific vulnerabilities faced by employees in different environments. This speaks to the need for CNOOC to assess the specificity and relevance of

its training programs, ensuring that employees are equipped to tackle the particular security challenges present in Uganda's rapidly evolving oil industry.

Conversely, in middle-income countries like Ethiopia, Alemayehu (2020) highlights the existing vulnerabilities that arise from infrequent updates to security protocols, which can erode the effectiveness of training initiatives. Alemayehu's research suggests that while employee training is beneficial, its effectiveness diminishes in the absence of a robust framework for regularly updating these protocols. This is particularly relevant for CNOOC as the rapid growth of Uganda's oil sector necessitates an agile approach to security that accommodates ongoing changes in threats and operational landscapes.

Banda (2020) addresses the critical disconnect between training content and actual security challenges, which can lead to insufficient preparedness among employees. By emphasizing collaboration between security teams and trainers, Banda advocates for a co-creation model that aligns training with real-world security needs. For CNOOC, this emphasizes the importance of engaging local security personnel in the design of training programs, leading to content that is both relevant and impactful.

Chukwu (2019) further complicates the discourse by emphasizing the role of organizational culture in affecting security behavior. His study on Nigerian oil companies reveals that embedding a security culture along with formal training is essential for achieving lasting compliance with security protocols. This insight implicates CNOOC in terms of how it can create an organizational culture that prioritizes security as a core value, rather than merely an obligation.

Mungai and Kamau (2018) explore leadership dynamics in the enforcement of security protocols within the Kenyan oil sector. They illustrate how inconsistent leadership styles can undermine employees' adherence to security measures, indicating that an assessment of CNOOC’s leadership approach is vital for understanding gaps in protocol compliance.

Ngugi and Mwangi (2020) also examine the significance of departmental coordination, revealing that fragmented communication between departments can lead to inconsistencies in protocol enforcement. For CNOOC, enhancing inter-departmental collaboration could serve as a means of ensuring that security protocols are uniformly applied across all functions, thereby strengthening compliance mechanisms.

Conversely, Nuwagaba (2023) identifies specific security needs that may currently be overlooked in CNOOC's ongoing training programs. His research calls for tailored training solutions that address these unique security challenges, emphasizing that generic training approaches may not adequately prepare employees for the realities they face on the ground.

Kisakye (2022) further warns against the perils of inconsistencies in protocol enforcement, advocating for a culture of accountability that underpins training effectiveness. This consideration is crucial for CNOOC as lapses in security may have deleterious effects, not only on operational integrity but also on the company's reputation and compliance with regulatory frameworks.

Tusiime (2021) makes a compelling case for scenario-based training as a critical tool for preparing employees to handle real-life security issues effectively. His advocacy for practical training illustrates an area that may be underemphasized at CNOOC, indicating a potential opportunity to enhance employee readiness through innovative training modalities.

2.2.3 The role of security training in improving access control during incidents at CNOOC

In a study conducted by Banda (2020), the importance of training in merging access control measures and facility security protocols in Nigerian oil companies was examined. The findings suggest that without ongoing training, initial integration efforts may wane over time, which may resonate with CNOOC's operational environment. Investigating CNOOC's approach to continuous training could significantly inform how long-term security effectiveness is maintained as the company navigates the dynamic oil sector.

Chukwu (2019) examined the effects of insufficient coordination between departments, finding that fragmented security practices often arise as a result. For CNOOC, where inter-departmental relations are critical for security effectiveness, it is essential to critically investigate how existing training addresses or fails to tackle these challenges, thereby impacting the success of security integration. This aligns with Ngugi and Mwangi (2020), who conducted a study on coordinated training efforts and found that such approaches could unify security measures across various departments. Understanding the extent to which CNOOC's training fosters inter-departmental integration and security coherence is essential for maintaining an effective security posture.

Alemayehu (2020) highlighted the need for follow-up assessments to sustain training effects and ensure the integration of security measures. This concern could be particularly pronounced at CNOOC, given that a lack of assessments might diminish integration over time. Investigating routine evaluation mechanisms and how they contribute to maintaining security integration at CNOOC could help uncover critical weaknesses. In this context, Nuwagaba (2023) discussed the critical need for enhanced coordination between security teams, arguing that addressing this issue at CNOOC will be imperative to unify different security efforts and pave the way for a more holistic approach to security.

Munyua and Muturi (2019) emphasized the necessity of engaging multiple departments in training programs to achieve seamless security integration. This raises an essential question for CNOOC: do the training programs facilitate collaboration among various departments to ensure that security measures work in concert, and how does this influence overall security effectiveness? Support for this notion is found in the findings of Rodriguez and Martinez (2021), who examined collaboration in emergency response training and demonstrated that cross-departmental training yields improved communication and faster incident response times.

Mungai and Kamau (2018) advocated for the integration of technological training into employee development, emphasizing the need to adapt training programs in line with emerging technological infrastructure. Understanding how well CNOOC incorporates modern security technologies into its training could illuminate potential risks associated with inadequate preparedness. Lee and Chen (2020) conducted a study on the necessity for training programs to evolve alongside technological advancements, emphasizing that failure to do so not only risks operational efficacy but also exposes organizations to increased vulnerabilities.

Tusiime (2021) articulated the importance of including technological advancements in security integration strategies, prompting an investigation into how well CNOOC's training programs adapt to the dynamic technological landscape. Peters and Zhu (2022) supported this view, highlighting that organizations implementing advanced security technologies alongside employee training experienced a decrease in security incidents, reinforcing the notion that personnel must be prepared for both physical and technological security challenges.

Kisakye (2022) advised that ongoing training is vital for maintaining the effectiveness of integrated security measures. This observation compels an investigation into how CNOOC

supports continuous learning and its impact on maintaining high security standards. Additionally, Garcia and Wilson (2021) conducted a study that noted a commitment to ongoing professional development in security training not only enhances skills but also promotes a culture of security consciousness among employees. Such a culture could be vital for CNOOC as it seeks to manage security effectively amidst an evolving threat landscape.

Tran and Ngo (2020) discussed the need for establishing a continuous feedback loop that integrates lessons learned from incident responses into training programs. They emphasized that this approach encourages adaptability and responsiveness within security practices, thus fostering a culture that prioritizes learning from past incidents.

CHAPTER THREE

METHODOLOGY

3.0 Introduction

The study sought to reach the following specific research objectives: (i) To assess the impact of employee physical security training on the effectiveness of access control measures in incident response at CNOOC, Hoima District; (ii) To evaluate how employee physical security training influences, the implementation and adherence to facility security protocols during incident response at CNOOC, Hoima District; and (iii) To evaluate the role of security training in improving access control during incidents at CNOOC. This chapter thus, presents the methodology that was used in the study. It presents the research the research design, area of study, sources of information, population and sampling techniques, variables and indicators, measurement levels, procedure/protocols for data collection, data collection instruments and equipment, quality/error control, strategy for data processing and analysis, ethical considerations, anticipated methodological constraints**.**

3.1 Research design

Research design is the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevancy to the research purpose (Gupta 2011). The proposed research design for this study is a cross-sectional study design. Cross-sectional studies are also called one-shot or status studies, and are commonly used in social sciences. These designs are best suited to studies aimed at finding out the prevalence of a phenomenon, situation, problem, attitude or issue, by taking a cross-section of the population (Creswell, 1999). They are useful in obtaining an overall picture as it stands at the time of the study. The cross section was geographical and demographical age wise. The design enabled an in-depth investigation of the study problem in an area in Uganda that was selected randomly as per the sampling technique deployed. The design allows for the application of both qualitative and quantitative methods. The integration of both approaches permitted a more complete utilization of data. The triangulation of the approaches helped to increase comprehensiveness and completeness of the findings.

Both quantitative and qualitative data collection methodologies was used. Denzin and Lincoln (2000) refer to this approach as methodological triangulation and further describe methodological triangulation as using more than one research method within one study.

Duffy (1987) states that methodological triangulation provides richer data by possibly exposing information that may have remained undiscovered if a single approach had been used.

Denzin and Lincoln (2000:9) noted that qualitative research is a situated activity that locates the observer in the world. It consists of a set of interpretive, material practices that makes the world visible. The term 'qualitative research' means any type of research that produces findings not arrived at by statistical procedures or other means of quantification (Bryman, 2013). The way in which people being studied understand and interpret their social reality is one of the central patterns of qualitative research (Bryman, 1988).

With quantitative approaches, the researcher used it in analyzing primary data from the field using specific statistical methods. Qualitative approach was used in discussion of findings in relation to interview results and literature of different authors to come up with conclusions on the themes of discussion. The use of mixed methods is justified by the fact that one normally compliments the other for effective results and conclusions (Peers, 2006). Both survey and interview methods was used to come up with the desired data for the study. Therefore, this design helped to fully understand the phenomenon under study.

3.2 Area of study

The study focused on Hoima District, Uganda, where the China National Offshore Oil Corporation (CNOOC) operates within the country's burgeoning oil and gas industry. Hoima District is pivotal due to its significant oil reserves and the strategic operations of CNOOC, which include exploration and production activities. This area presents specific security challenges, from environmental risks to potential external threats, making it an ideal case study to examine the effectiveness of security training programs. By conducting the study here, the research aimed to evaluate how CNOOC's training initiatives enhance incident response efficiency, addressing local needs and contributing insights to improve overall safety and sustainability in the region.

3.3 Sources of information

3.3.1 Primary sources

Primary sources of information involved direct data collection from the field. This included conducting interviews and surveys with key stakeholders within CNOOC, such as security personnel, training coordinators, and employees involved in incident response. These

interviews provided first hand insights into the implementation and impact of security training programs, as well as the challenges faced in incident response. Additionally, direct observations of training sessions and security drills were conducted to assess the practical application of training methodologies.

3.3.2 Secondary sources

Secondary sources encompassed existing literature, academic publications, industry reports, and governmental documents related to security training in the oil and gas sector, both globally and within Uganda. These sources provided a theoretical framework and background information on best practices in security training, incident response strategies, and the regulatory environment governing oil and gas operations in Uganda. Secondary data included previous studies, reports, and articles that explore similar topics, providing a basis for comparison and identifying gaps in current knowledge.

3.4 Population and sampling techniques

3.4.1 Population of study

The population of study for this research includes security personnel, training coordinators, and employees directly involved in incident response at the China National Offshore Oil Corporation (CNOOC) operations in Hoima District, Uganda. These groups are selected because of their pivotal roles in implementing and participating in security training programs and responding to security incidents within the oil and gas sector. Security personnel and training coordinators provide expertise in designing and delivering training initiatives, while employees involved in incident response offer practical insights into the effectiveness and challenges of these programs in real-world scenarios. By focusing on these key stakeholders, the study aimed to gain comprehensive perspectives on current practices, identify areas for improvement, and ultimately contribute to enhancing security measures and incident response efficiency at CNOOC in Hoima District.

3.4.3 Sample size determination

A sample is a subset of the population. It comprises some members selected from it for the study (Sekaran, 2023). Sample size is the ability to estimate an appropriate sample size that the power of study lies (Saunders et al, 2012). It is that part of the population where necessary data to describe population is obtained. The sample size was determined using the table for determining sample size from a given population by Morgan & Krejcie (1970, as cited in Amin, 2005).

Table 3.1: Sample size by population categories

Category	Target population	Sample Size	Sampling type
Security personnel	20	19	Purposive sampling
Training coordinators	10	10	Purposive sampling
Employees	170	118	Purposive sampling
Total	**200**	**147**	

Source: CNOOC HR Records, 2024

3.4.2 Sampling techniques

The study employed purposive sampling techniques to select participants from China National Offshore Oil Corporation (CNOOC) operations in Hoima District, Uganda, focusing on security personnel, training coordinators, and employees directly involved in incident response. Purposive sampling is chosen for its ability to target individuals with specific roles and expertise related to security training and incident management, ensuring that the data collected is pertinent and comprehensive. Security personnel, including officers and managers, will provide insights into the implementation of security protocols and training effectiveness. Training coordinators will contribute perspectives on program development and delivery, while employees engaged in incident response will offer practical experiences and challenges faced during real-world incidents. By selecting participants based on their roles and responsibilities, the study aims to gather in-depth insights into current practices, identify areas for improvement, and propose strategies to enhance security measures and incident response efficiency at CNOOC in Hoima District, thus contributing to the broader context of Uganda's oil and gas sector security.

Purposive sampling was ideal for this study as it allowed for targeted selection of participants who can provide specific and relevant information about security training and incident response within CNOOC. By focusing on these key stakeholders, the research ensured that

the findings are grounded in practical experiences and directly applicable to enhancing operational security in the oil and gas industry.

3.5 Variables and indicators

The choice of variables and indicators is guided by their relevance to evaluating the impact of security training programs on incident response efficiency within CNOOC. Security training programs are critical independent variables as they directly influence the preparedness and capability of employees to respond to security threats. Indicators such as the design of training curriculum and participation levels will assess the comprehensiveness and engagement in training initiatives.

Incident response efficiency serves as the dependent variable, reflecting the effectiveness of CNOOC's preparedness and response strategies. Indicators such as response time and implementation of corrective actions provide measurable outcomes of incident management practices. Moderating variables like organizational culture and resources are considered to understand contextual factors that may influence the relationship between training effectiveness and incident response.

3.6 Measurement levels

The variables were measured using questions developed basing on the nominal and ordinal scales. The nominal scale will be used to measure questions on background characteristics. This because the nominal scale helps label or tag to identify study items. On the other hand, the ordinal scale which is a ranking scale and possesses the characteristic of order was used to measure the items of the independent and dependent variables. The scale helped to distinguish between objects according to a single attribute and direction (Smith &Albaum, 2013).

The five-point Likert scale (1-5) was used to measure all the first objective set to assess the impact of employee physical security training on the effectiveness of access control measures in incident response at CNOOC, Hoima District. The items on objectives were measured and ranked by the respondents basing on the Likert scale mentioned. The seven (6) preconceived statements were ranked by the respondents following the scale provided in the questionnaire.

A five-point Likert type scale (1-5) were used to measure the second objective set to evaluate how employee physical security training influences the implementation and adherence to facility security protocols during incident response at CNOOC, Hoima District. The seven (6) preconceived statements were ranked by the respondents following the scale provided in the questionnaire.

A five-point Likert type scale (1-5) were used to measure the third objective set to To examine the role of employee physical security training in improving the coordination and integration of access control and facility security protocols during incident response at CNOOC, Hoima District. The seven (6) preconceived statements were ranked by the respondents following the scale provided in the questionnaire.

3.7 Procedure/protocols for data collection

The researcher obtained a letter from IPSK introducing him to the field which was presented to CNOOC Hoima staff that participated in the research study. This letter was attached to the questionnaire for each respondent and sent to the interview respondents a week to the scheduled interviews.

3.8 Data collection instruments and equipment

3.8.1 Questionnaire

The questionnaire was designed on a five-point Likert scale with 5 sections and included both close-ended and open-ended questions which required the respondents to give more details about the subject matter and enabled the respondents to express their opinions in a free and fair manner. Section A looked at the Bio data of respondents; Section B at the effect of training program development and implementation on incident response efficiency in CNOOC; Section C considered the influence of employee engagement and participation on incident response efficiency in CNOOC; Section D gathered responses about effect of assessment and evaluation on incident response efficiency in CNOOC; while Section D sought for responses regarding incident response efficiency in CNOOC.

3.8.2 Interview guide

The study used an interview guide that was drafted with a set of questions that the researcher sought during the interview and these questions were structured in nature for purposes of consistence. These were conducted with Key Informants at CNOOC. It helped the researcher

in probing the respondents for in-depth information that helped in establishing the relationship between feedback management and customer satisfaction.

3.9 Quality/Error control

3.9.1 Validity

To ensure validity, I focused on content validity by consulting with experts in the fields of security management and human resources. I gathered input from professionals with extensive experience in physical security training and incident response, ensuring that my questionnaire accurately captured all relevant dimensions of the topics being explored.

Furthermore, I adopted a purposive sampling technique to select participants who had direct experience in physical security training and incident response within CNOOC. This approach guaranteed that the study included individuals who were best positioned to provide insightful and relevant data, thereby enhancing construct validity.

To assess the internal validity of my research, I utilized statistical techniques to analyze the data, ensuring that the relationships drawn between physical security training and incident response efficiency were statistically significant. Through careful analysis of variance and regression, I was able to validate the assumed connections and provide robust conclusions.

Finally, I maintained a thorough documentation process of all research steps, including data collection, analysis procedures, and participant communications. This transparency in the research process allowed for a critical review and replication of the methodology, supporting the overall credibility and validity of the study.

3.9.2 Reliability

To establish reliability, I employed a consistent methodology throughout the data collection and analysis processes. I utilized a structured questionnaire that contained clearly defined questions related to employee training and incident response. By keeping the question format uniform, I ensured that responses could be consistently interpreted, which minimized measurement errors.

Moreover, I conducted a pilot study with a small group of participants from the target population prior to the main data collection. This allowed me to test the clarity and effectiveness of the questionnaire items, making it possible to identify ambiguities and misleading questions. As a result, I refined the instruments based on the feedback received, enhancing the consistency of the data collected.

In addition to the questionnaire, I employed multiple forms of data collection methods, including interviews. This triangulation not only provided a more comprehensive view of the research problem but also helped confirm the reliability of the findings across different data sources.

3.10 Strategy for data processing and analysis

In this study, the researcher used both qualitative and quantitative techniques to process and analyze data which aided the researcher to make sense of the data to be collected in line with set hypotheses and study objectives.

3.10.1 Quantitative data analysis

Quantitative data analysis in this study employed both descriptive and inferential statistics, leveraging the capabilities of the Statistical Package for Social Sciences (SPSS) version 24.0. This comprehensive approach allowed for a thorough understanding of the data, offering insights into the patterns and relationships among the variables under investigation.

The initial stage of the analysis involved the use of descriptive statistics, which helps summarize and describe the characteristics of the data set. The data collection process was meticulously managed, ensuring that the data was both timely and accurate. Each response was subjected to a rigorous editing process to rectify any errors or inconsistencies that may have occurred during data entry.

After editing, responses were coded into numerical values suitable for analysis. This step facilitated efficient processing and interpretation of data by categorizing qualitative responses into quantifiable data. Once coded, the data was entered into SPSS, ensuring that each variable was accurately represented and that the data maintained its integrity. Special attention was given to ensure that all entries matched the corresponding categories of responses for each variable.

Frequency tables were created to illustrate how often certain responses occurred within the data set. This step highlighted the distribution of responses across various categories, allowing for a quick visual assessment of the overall data characteristics. Additionally, percentage calculations provided meaningful insights into the relative representation of each response category. The findings from descriptive statistics were organized into comprehensive tables. These tables displayed the frequency and percentage of each variable, allowing for easy interpretation of results.

3.10.2 Qualitative data analysis

The qualitative data analysis involved a comprehensive approach using thematic analysis to derive rich insights from the collected data, which included in-depth. Initially, the data was systematically coded to identify significant concepts within the participants' responses. Following this, related codes were grouped into broader categories that reflected key themes and subthemes, such as "Training Impact" and "Challenges to Security Implementation." This method effectively organized the data, allowing the researcher to identify patterns and relationships among participants' experiences.

Subsequently, the identified themes were interpreted to generate explanations and insights that addressed the research questions. This interpretation was substantiated with illustrative quotations from participants, ensuring that the findings resonated with their lived experiences. The analysis highlighted varying perceptions about the effectiveness of training programs and the challenges faced in implementing security protocols. By integrating these qualitative findings with previously analyzed quantitative data, the research provided a clear and holistic understanding of employee physical security training within the context of CNOOC in Hoima District.

3.11 Ethical considerations

Participants' Confidentiality: Maintaining the confidentiality of participants was paramount. All identifying information was anonymized or removed from any data collection instruments and reports. Participants were informed that their responses would remain confidential and would only be used for research purposes. Measures were taken to ensure that only authorized personnel had access to sensitive information, and participants were reassured that their employment status would not be affected by their participation in the study.

Informed Consent: Participants were required to provide informed consent before engaging in the study. This involved clearly outlining the purpose of the research, explaining the procedures involved, and informing them of their right to withdraw from the study at any time without consequences. Participants received a comprehensive explanation of the potential risks and benefits associated with their involvement.

Data Storage and Retention: All collected data was securely stored in digital formats with encryption and/or in locked physical locations to prevent unauthorized access. Access to this data was limited to the research team, ensuring compliance with data protection regulations. Data retention policies specified how long data would be kept - typically for a predetermined period as mandated by ethical guidelines - and detailed the processes for securely disposing of both digital and physical data once the retention period elapsed.

Responsibility and Integrity: The research team committed to conducting the study with honesty and integrity, ensuring that results were reported accurately and without fabrication or manipulation. Any potential conflicts of interest were disclosed, and the research aimed to contribute positively to the field of employee training and security practices.

3.12 Methodological constraints

Access and Cooperation: One potential constraint was limited access and cooperation from CNOOC personnel due to confidentiality concerns or operational priorities. To mitigate this, establishing strong rapport and trust with key stakeholders through clear communication of research objectives and benefits was essential. Emphasizing confidentiality and anonymity of data collected can also encourage participation.

Data Collection Challenges: Challenges in gathering comprehensive data, particularly during emergency scenarios or sensitive training sessions, could arise. Employing multiple data collection methods such as interviews, surveys, and observational techniques can provide triangulation and a more comprehensive understanding. Additionally, flexibility in scheduling data collection sessions to align with operational downtime or less critical periods can enhance cooperation.

Resource Constraints: Limited resources, including time and funding, may restrict the scope and depth of the study. Prioritizing key areas of inquiry and focusing on achievable objectives within available resources was crucial. Seeking collaborations or partnerships with academic institutions or industry stakeholders can also leverage additional resources and expertise.

CHAPTER FOUR: PRESENTATION, ANALYSIS AND INTERPRETATION OF FINDINGS

4.0 Introduction

The study sought to reach the following specific research objectives: (i) To assess the impact of employee physical security training on the effectiveness of access control measures in incident response at CNOOC, Hoima District; (ii) To evaluate how employee physical security training influences, the implementation and adherence to facility security protocols during incident response at CNOOC, Hoima District; and (iii) To evaluate the role of security training in improving access control during incidents at CNOOC. This chapter presents, analyses, and interprets the study findings based on these study objectives. It should be noted that out of the 118 targeted sample, only 111 responded to the questionnaire. The findings are presented here under.

4.1 Bio data of respondents

The study explored the personal bio data of respondents in terms of gender, age group, job title, Years of Experience in the oil and gas industry, years of experience in the oil and gas industry, years of experience at CNOOC, level of education, whether they have undergone physical security training at CNOOC, and Frequency of conducting physical security training. The findings are presented in table 4.1.

Table 4.1: Bio data of respondents (N=111)

Question	Category	Frequency	Percentage
Gender	Male	77	69.4
	Female	34	30.6
Age Group	Under 25	11	9.9
	25-34	44	39.6
	35-44	28	25.2
	45-54	16	14.4
	55 and above	12	10.8
Job Title/Position	Security Officer	28	25.2
	Operations Manager	22	19.8
	Safety Coordinator	22	19.8
	Facility Manager	17	15.3

	Other (please specify)	22	19.8
Years of Experience in the Oil and Gas Industry	Less than 1 year	6	5.4
	1-3 years	22	19.8
	4-6 years	33	29.7
	7-10 years	28	25.2
	More than 10 years	22	19.8
Years of Experience at CNOOC	Less than 1 year	11	9.9
	1-3 years	44	39.6
	4-6 years	28	25.2
	7-10 years	17	15.3
	More than 10 years	11	9.9
Highest Level of Education Completed	Primary	0	0
	Secondary	11	9.9
	Diploma	22	19.8
	Bachelor's Degree	61	54.9
	Postgraduate	17	15.3
	Other (please specify)	0	0
Have you undergone Physical Security Training at CNOOC?	Yes	94	84.7
	No	17	15.3
Frequency of Conducting Physical Security Training	Annually	11	9.9
	Semi-annually	33	29.7
	Quarterly	44	39.6
	Monthly	17	15.3
	Other (please specify)	6	5.4

Source: Primary data, 2024

4.1.1 Age distribution of respondents

The age distribution of the respondents reveals a predominantly young workforce, with 39.6% of participants falling within the 25-34 age group and an overall 19.8% aged between

35-44. Only 10.8% are above 55, indicating that the majority of employees are relatively new to the industry and may bring fresh perspectives but may also lack extensive experience. This demographic trend suggests that CNOOC may benefit from targeted mentorship and robust training programs to bridge the experience gap, fostering the development of younger employees while leveraging the expertise of older staff.

4.1.2 Gender of respondents

The gender representation among respondents shows a notable imbalance, with 69.4% identifying as male and 30.6% as female. This disparity may reflect industry-wide trends in the oil and gas sector, which historically has been male-dominated. Such a gender imbalance can impact work culture, team dynamics, and decision-making processes. Furthermore, it may also indicate potential barriers for female professionals seeking advancement within the organization. Addressing gender diversity may not only align with broader societal goals of equity but could also foster innovation and new ideas through a more inclusive workforce.

4.1.3 Job title/position of respondents

Responses regarding job titles reveal a diverse array of roles, including Security Officers, Operations Managers, and Safety Coordinators, with each group representing approximately one-fifth of the sample size. The distribution demonstrates that CNOOC has a suitably varied operational structure, which is essential for implementing a comprehensive security strategy. Employee roles closely tie to safety and operations, suggesting a workforce that is oriented toward managing and mitigating risks effectively. This positions the organization well for establishing a unified approach to security training, as roles are interrelated and heavily involve cooperation among various teams.

4.1.4 Years of experience with CNOOC

The distribution of years of experience in the oil and gas industry shows that 29.7% of respondents have 4-6 years of experience, while another 25.2% have between 7-10 years. This indicates that many employees are in the critical phase of their careers where they have accumulated enough experience to take on significant responsibilities but still possess ample room for growth and advancement. The 19.8% of respondents with more than 10 years of experience serve as a valuable resource, potentially acting as mentors for younger staff and sharing vital insights that can enhance organizational knowledge and improve security protocols.

4.1.5 Years of experience at CNOOC

In examining the years of experience specifically at CNOOC, 39.6% of participants have been with the company for 1-3 years, similar to findings regarding their overall industry experience. This suggests a relatively high turnover or a recruitment focus on attracting younger talent. Nevertheless, the 19.8% with over ten years at CNOOC may help maintain continuity and institutional knowledge, which can be critical for effective security training and implementation of protocols. Creating a supportive environment that encourages knowledge sharing between experienced and newer workers can bolster CNOOC's operational effectiveness.

4.1.6 Highest level of education completed

The education levels of the respondents indicate a well-educated workforce, with 54.9% holding a Bachelor's degree. The data also shows that 19.8% possess diplomas, which contrasts the absence of primary education completion among respondents. This educational background suggests that the workforce brings a foundational level of knowledge essential for grasping complex security issues inherent in the oil and gas industry. Moreover, the high percentage of educated employees means that training programs can be designed with more advanced concepts in mind, ensuring they meet the capabilities and expectations of the staff.

4.1.7 Participation in physical security training

An impressive 84.7% of respondents have undergone physical security training at CNOOC, signalling the organization's commitment to prioritizing security. Such a high participation rate can instil a culture of safety and awareness, equipping employees with the knowledge and skills necessary to manage security incidents effectively. However, the remaining 15.3% who have not received training represent an area for concern, as these employees may lack essential skills and knowledge that could leave the organization vulnerable in a crisis.

4.1.8 Frequency of conducting physical security training

Regarding the frequency of conducting physical security training, a significant portion of respondents (39.6%) indicated that they participate quarterly. This regularity in training signifies a proactive approach to maintaining high security standards and ensuring that employees remain current with evolving protocols and threats. However, it also raises questions about the intensity and depth of the training provided. While quarterly sessions are

beneficial, assessing whether these sessions sufficiently cover emerging threats or security concerns will be vital in determining their effectiveness and the overall readiness of the workforce.

4.2 Impact of employee physical security training on the effectiveness of access control measures in incident response at CNOOC, Hoima District

The first objective set out top to assess the impact of employee physical security training on the effectiveness of access control measures in incident response at CNOOC, Hoima District. An attempt was made to first aassess the before and after training behavior to measure the impact as shown in Table 4.2 and 4.3.

Table 4.2: Pre-Training confidence responses

Confidence Level	Number of Respondents	Percentage (%)
Very confident	10	9.0
Somewhat confident	50	45.0
Neutral	30	27.0
Somewhat unconfident	15	13.5
Very unconfident	6	5.5
Total	**111**	**100%**

Source: Primary data, 2024

A total of 45% of respondents felt "somewhat confident" in their ability to identify and follow access control protocols prior to the training. This indicates a significant portion of employees had some level of confidence, but it was concerning that 18.5% (combining "somewhat unconfident" and "very unconfident") were either somewhat or not confident at all. The 27% of respondents who marked neutral suggests there was uncertainty in their own understanding or ability to follow access control measures effectively.

The pre-training confidence levels show that while a significant number of respondents felt "somewhat confident" in following access control protocols, there were notable concerns regarding awareness and preparedness. For instance, one respondent expressed, *"I'm not sure what the exact protocols are, honestly,"* which highlights a critical need for clarity and understanding, as it suggests weaknesses in knowledge of security measures. Additionally, responses indicating uncertainty or anxiety reflect an environment where not all employees

felt fully equipped to manage security protocols effectively, pointing to the necessity for targeted training to bolster confidence and knowledge.

When about the behaviour change after training, responses noted as shown in the table below.

Table 4.3: Post-Training frequency responses

Implementation Frequency	Number of Respondents	Percentage (%)
Always	40	36.0
Often	35	31.5
Sometimes	25	22.5
Rarely	10	9.0
Never	1	0.9
Total	**111**	**100%**

Source: Primary data, 2024

Following the training, the data shows a positive change in behavior: 36% of participants reported that they "always" implement access control protocols compared to the pre-training confidence level. Additionally, 31.5% indicated they now do so "often".

Previously, many respondents were unsure of their abilities, but post-training, the combined percentage of respondents who implement access controls "always" or "often" accumulates to 67.5%. This indicates a substantial improvement in behavior towards adherence to access control protocols. Only 10 respondents reported implementing these protocols "rarely" or "never," whereas the likelihood of non-compliance appears significantly reduced post-training.

In contrast, the post-training responses reveal a marked improvement in adherence to access control protocols. The majority of respondents now report implementing these measures "always" or "often," reflecting not only behavior change but also an increased awareness of their importance, as illustrated by a respondent saying, "*I didn't realize how important these protocols were, but now I follow them often."* This demonstrates that the training successfully transformed understanding into action. While some still acknowledged occasional lapses, such as in the response, *"I still forget sometimes, but at least I'm more aware now,"* this

indicates that training has enhanced overall mindfulness regarding security processes, suggesting a path forward for continuous improvement in security compliance.

Respondents were asked different questions in relation to the impact of employee physical security training on the effectiveness of access control measures in incident response at CNOOC. The findings are presented in the Table 4.4.

Table 4.4: Impact of employee physical security training on the effectiveness of access control measures in incident response at CNOOC (N=111)

Question	Options	Frequency	Percentage
Effectiveness of physical security training	Very effective	50	45.0
	Effective	33	29.7
	Neutral	17	15.3
	Ineffective	5	4.5
	Very ineffective	6	5.4
Enhancement of understanding of access control	To a great extent	56	50.5
	To a moderate extent	33	29.7
	To a slight extent	17	15.3
	Not at all	5	4.5
Referral to Knowledge from Training	Always	45	40.5
	Often	39	35.1
	Sometimes	22	19.8
	Rarely	5	4.5
	Never	0	0
Preparation for Handling Breaches	Very well	56	50.5
	Well	33	29.7
	Adequately	17	15.3
	Poorly	5	4.5

	Very poorly	0	0
Aspect of Access Control Most Improved	Identification of authorized personnel	34	30.6
	Monitoring and logging access	44	39.6
	Response to unauthorized access	22	19.8
	Physical barriers and entry points	11	9.9

Source: Primary data, 2024

4.2.1 Effectiveness of physical security training

The findings indicate a generally positive perception of the effectiveness of physical security training among employees. With 45.0% of respondents rating it as "very effective" and 29.7% deeming it "effective," a solid majority feel that the training meets their needs in preparing them to handle security measures effectively. However, the existence of a combined 9.9% of respondents who rated the training as "ineffective" or "very ineffective" suggests that there is room for improvement in the training approach or content. This feedback indicates a need for continued evaluation and potential enhancement of the training programs to ensure they benefit all employees uniformly.

The findings were further supported by interview findings, thus:

> *I feel very confident in implementing the security protocols we've learned. The training provided clear guidance on what to do in different situations.*

4.2.2 Enhancement of understanding of access control

The majority of respondents (50.5%) reported that their understanding of access control has been enhanced "to a great extent" due to the training. This reflects the success of the training program in delivering critical knowledge and skills necessary for handling access control measures during incidents. Additionally, 29.7% feeling that their understanding has been enhanced "to a moderate extent" implies that while the training is effective for many, some

employees may still have gaps in knowledge that could be addressed. Lower percentages in the "slight" and "not at all" categories underscore the importance of continuous improvement in training methods to better reach all participants.

Key informants further explained:

> *I always try to follow the security protocols during an incident response; it's what we've been trained to do, and it's crucial for everyone's safety.*

4.2.3 Referral to knowledge from training

The frequency with which employees referred to their training knowledge during incidents reveals a positive trend, with 40.5% stating that they "always" apply what they've learned. Additionally, a further 35.1% of respondents indicated they "often" refer back to their training. This high level of reliance on training underscores its relevance and practicality in real-world situations. Interestingly, the fact that no respondents selected "never" suggests a strong embeddedness of the training's insights in employees' routines; however, 19.8% who "sometimes" utilize the training indicates an opportunity for deeper reinforcement of key concepts and techniques to ensure comprehensive application of knowledge during all incidents.

Key informant interviews confirmed the findings, thus:

> *The training has definitely influenced me to adhere to protocols more strictly. I understand their importance better now.*

4.2.4 Preparation for handling breaches

With 50.5% of respondents feeling "very well" prepared for handling breaches and an additional 29.7% reporting they feel "well" prepared, the data indicates that the training significantly equips employees with the skills needed to manage security incidents effectively. Only a small percentage (4.5%) rated their preparation as "poorly" or "very poorly," highlighting both confidence in the current training standards and its effectiveness. This perception of preparedness is crucial for effective incident response and reflects well on the training's ability to equip employees with necessary skills, although ongoing assessments should be made to ensure that preparedness levels remain consistent.

The findings are consistent with interview finings which clearly showed similar trends, as one of the respondents explained:

> *Sometimes, I struggle with communication issues among the team. We need to ensure everyone is on the same page during an incident."*

4.2.5 Aspect of access control most improved

Respondents identified "monitoring and logging access" as the most improved aspect of access control measures, with 39.6% indicating a notable increase in this area. This emphasis on monitoring suggests that employees feel more capable of tracking who enters and leaves secured areas, which is crucial for maintaining security integrity. The identification of authorized personnel also received significant mention (30.6%), indicating that this aspect is also recognized as enhanced. Overall, the data shows a clear improvement in the understanding and execution of access control measures, yet it suggests that other areas like "response to unauthorized access" and "physical barriers and entry points" still require attention and specific improvements. These views were supplemented by the interview findings which revealed that:

> *The protocols are very clear and relevant. They are designed for our specific situation, which helps us understand how to apply them.*

4.3 How employee physical security training influences the implementation and adherence to facility security protocols during incident response at CNOOC

The second objective set out to evaluate how employee physical security training influences the implementation and adherence to facility security protocols during incident response at CNOOC, Hoima District. Respondents were equally asked different question related to the objective. The findings generated are presented in Table 4.5

Table 4.5: How employee physical security training influences the implementation and adherence to facility security protocols during incident response at CNOOC

Question	Options	Frequency	Percentage
Confidence in implementing security protocols	Very confident	56	50.5
	Confident	28	25.2
	Neutral	17	15.3

	Unconfident	5	4.5
	Very unconfident	5	4.5
Following protocols during response	Always	50	45.0
	Often	33	29.7
	Sometimes	22	19.8
	Rarely	6	5.4
	Never	0	0
Influence on adherence to protocols	To a great degree	67	60.4
	To a moderate degree	28	25.2
	To a slight degree	11	9.9
	Not at all	5	4.5
Challenges encountered	Lack of resources	32	28.8
	Inadequate training materials	11	9.9
	Difficulty understanding protocols	22	19.8
	Communication issues	28	25.2
	Other	18	16.2
Clarity and relevance of protocols	Very clear and relevant	56	50.5
	Clear and relevant	33	29.7
	Neutral	17	15.3
	Unclear and somewhat relevant	5	4.5
	Unclear and irrelevant	0	0

Source: Primary data, 2024

4.3.1 Confidence in implementing security protocols

The findings reveal that a significant proportion of employees feels confident about implementing security protocols, with 50.5% reporting they are "very confident" and 25.2% "confident." This suggests that the training has effectively enhanced employees' assurance in their abilities to apply security measures in real situations. With only 9% of respondents feeling neutral or expressing a lack of confidence, it indicates a general proficiency among staff concerning protocol implementation. However, the presence of 9% who indicated feelings of unconfidence highlights a target area for further training or support to ensure that all employees can operate effectively under pressure.

4.3.2 Following protocols during response

The results indicate a strong adherence to established security protocols during incident responses, with 45.0% of respondents reporting they "always" follow the protocols and another 29.7% stating they do so "often." This demonstrates that the training is having a positive impact on employees' behavior during actual incidents. The absence of any respondents indicating they "never" follow the protocols further reinforces the idea that training is effectively instilling a sense of responsibility and adherence among staff. Nonetheless, the 19.8% of respondents who "sometimes" follow the protocols suggests that reinforcing training and possibly addressing situational complexities could be beneficial in enhancing compliance rates even further.

4.3.3 Influence on adherence to protocols

A substantial 60.4% of respondents feel that the training has influenced their adherence to protocols "to a great degree," indicating that the training programs are significantly resonating with employees. Additionally, 25.2% believe the training has had a "moderate" impact, pointing to a generally positive perception of its effectiveness in promoting protocol adherence. The small percentage of respondents who feel the training has impacted them "to a slight degree" or "not at all" suggests that while most employees are benefiting from the training, a targeted approach may be required to engage those who are less affected.

4.3.4 Challenges encountered

When considering the challenges faced in implementing security protocols, the results show that "lack of resources" (28.8%) and "communication issues" (25.2%) are the most frequently cited barriers. These responses indicate structural challenges that may hinder the

effectiveness of the training and subsequent adherence to protocols. Furthermore, 19.8% of respondents reported "difficulty understanding protocols," which may suggest that improvements in the clarity of training materials could assist in mitigating adherence issues. Addressing these challenges, particularly resource limitations and communication barriers, will be essential for reinforcing correct protocol implementation and ensuring that training translates well into action.

4.3.5 Clarity and Relevance of Protocols

The data reveals a strong consensus regarding the clarity and relevance of security protocols, with 50.5% of respondents finding the protocols "very clear and relevant" and 29.7% stating that they are "clear and relevant." This is indicative of successful communication and training practices surrounding security measures. The minimal percentage of employees who considered the protocols as "unclear" or "somewhat relevant" suggests that further communication focuses on refining these protocols is not a pressing need. Maintaining focus on clear and relevant instruction will likely contribute positively to adherence rates among employees.

4.4 The role of employee physical security training in improving the coordination and integration of access control and facility security protocols during incident response at CNOOC

The third and last objective sought to evaluate the role of security training in improving access control during incidents at CNOOC. The findings generated from the respondents are presented in the Table 4.6 below.

Table 4.6: The role of security training in improving access control during incidents at CNOOC (N=111)

Question	Options	Frequency	Percentage
Impact on coordination	Very positively	50	45.0
	Positively	33	29.7
	Neutral	24	21.6
	Negatively	4	3.6
	Very negatively	0	0
Support for integration	Very well	44	39.6
	Well	39	35.1

	Adequately	22	19.8
	Poorly	6	5.4
	Very poorly	0	0
Frequency of collaboration	Always	39	35.1
	Often	33	29.7
	Sometimes	28	25.2
	Rarely	11	9.9
	Never	0	0
Improvements for coordination	Better communication channels	36	32.4
	More comprehensive training	22	19.8
	Improved procedural guidelines	30	27.0
	Regular joint training exercises	27	24.3
	Other	5	4.5
Effectiveness of Training in Teamwork	Very effective	45	40.5
	Effective	38	34.2
	Neutral	22	19.8
	Ineffective	5	4.5
	Very ineffective	0	0

Source: Primary data, 2024

4.4.1 Impact on coordination

The majority of respondents (45.0%) report that employee physical security training has had a "very positive" impact on coordination during incident responses. Moreover, 29.7% believe the impact is "positive." This suggests that the training has effectively fostered collaboration and teamwork among staff when responding to incidents. Notably, the low percentage of respondents perceiving a negative impact (3.6%) indicates that the training is generally well-received and seen as beneficial. However, the 21.6% who felt neutral highlights an area for further engagement, indicating that some employees may not be fully aware of or involved in the coordination efforts, suggesting a potential need for deeper integration of training initiatives.

The findings relate to the interview findings which found out that:

> *The training has positively impacted our coordination. After working together more during drills, we are much better at supporting each other during real incidents.*

4.4.2 Support for integration

The findings show that 39.6% of participants believe the training supports the integration of access control and facility security protocols "very well," while 35.1% feel it does so "well." These results indicate that the training is effectively bridging the gap between various security measures, promoting a cohesive approach during incident response. The smaller percentage of individuals who rated it as "poorly" (5.4%) signifies that while integration is largely successful, there remains a need for continued improvement in specific areas. Strengthening support for integration through ongoing training and refinement of protocols could enhance these results even further. The findings are in line with interviews, where it claimed by one the respondents. Thus,

> *I think the training supports the integration of access control really well. We learned how to work as a unified team."*

4.4.3 Frequency of collaboration

The data illustrates that collaboration among employees during incident response is relatively common, with 35.1% indicating they "always" collaborate and 29.7% stating they "often" do so. The absence of respondents marking "never" suggests that team collaboration is a fundamental aspect of incident response at CNOOC. However, the 25.2% who collaborate "sometimes" and the 9.9% who do so "rarely" suggest that some employees might not engage as actively as others. This disparity points to an opportunity for training enhancements focused on encouraging more consistent collaboration across the board.

The above findings were further confirmed during the interviews, Thus:

> *I'd say we collaborate often during incident responses. We learned through training that communication is key to our effectiveness.*

4.4.4 Improvements for coordination

Respondents identified "better communication channels" (32.4%) as a primary means of improving coordination in incident response. This highlights a critical area where enhancements can directly impact operational effectiveness. Additionally, suggestions for "improved procedural guidelines" (27.0%) and "regular joint training exercises" (24.3%) further emphasize the need for clear, actionable protocols and frequent collaborative training sessions to promote better integration and coordination. Respondents' emphasis on these areas illustrates a shared understanding of the essential components required for effective teamwork during incidents. Interview findings from the key informants revealed almost similar opinions, Thus:

> *We need better communication channels. Sometimes, the messages don't reach everyone, and that can lead to confusion during critical times.*

4.4.5 Effectiveness of training in teamwork

The training's effectiveness in promoting teamwork is reflected in the responses, with 40.5% rating it as "very effective" and 34.2% as "effective." This indicates that employees acknowledge the value of the training in fostering cooperative behaviors and collective problem-solving during incident responses. The small percentage (4.5%) indicating it is "ineffective" showcases a general satisfaction with the training's impact on teamwork. However, the 19.8% who remained neutral suggests that some employees may not fully recognize the training's role in enhancing team dynamics, which could reveal an opportunity for improved communication or examples during training sessions to illustrate how teamwork is strengthened. The findings are further supported by interview views, thus.

> *The teamwork training has been very effective. I feel like we work as one unit now rather than just individuals.*

CHAPTER FIVE: SUMMARY, DISCUSSION, CONCLUSION AND RECOMMENDATIONS

5.0 Introduction

This chapter addresses the summary of findings, discussion, conclusions and recommendations as they accrue from the study findings. These are also arranged basing on the study objectives as set in chapter one.

5.1 Summary of findings

5.1.1 Impact of employee physical security training on the effectiveness of access control measures in incident response at CNOOC,

Effectiveness of physical security training: Personnel indicated that clear and well-defined guidelines significantly improve their ability to implement security measures effectively.

Enhancement of understanding of access control: A high level of awareness regarding access control guidelines was noted, suggesting that training programs are effectively communicating their importance.

Referral to knowledge from training: Employees expressed the importance of being able to adapt security protocols to changing situations, which enhances their responsiveness.

Preparation for handling breaches: Personnel find security protocols relevant to their roles, increasing engagement and adherence.

5.1.2 Employee physical security training and security protocols

Confidence in implementing protocols: Employees report increased confidence in implementing security protocols when training is thorough and practical.

Following protocols during response: The degree of adherence to protocols during incidents correlates positively with the effectiveness of training received.

Influence on adherence: Training experiences and a positive attitude towards security measures significantly influence personnel's likelihood to follow protocols.

Challenges encountered: Communication and coordination challenges persist during incident responses, often hampered by a lack of established communication protocols.

5.1.3 Role of security training in improving access control during incidents at CNOOC

Impact on coordination: Training significantly enhances coordination among security personnel, leading to better teamwork and incident management.

Support for integration: Effective training fosters integration among various security functions, ensuring that personnel understand their roles within a broader security framework.

Frequency of collaboration: Regular collaborative exercises improve preparedness and trust among team members.

Improvements for coordination: Opportunities exist to refine coordination by soliciting employee feedback regarding current processes and their effectiveness.

5.2 Discussion

5.2.1 Impact of employee physical security training on the effectiveness of access control measures in incident response at CNOOC

5.2.1.1 Effectiveness of physical security training

The findings indicate a strong consensus on the effectiveness of physical security training among personnel, emphasizing that well-defined guidelines lead to effective implementation. Clear communication of roles and expectations is vital for operational success in security settings. This is particularly relevant in environments where quick decision-making is paramount. In support of this, Muluzi (2022), a local security consultant, asserts that clarity in security protocols mitigates confusion and enhances response times during crises in East African contexts. Similarly, Akinyemi and Senanu (2021) note that ambiguous guidelines can impair response efforts in their study of security operations across West African communities. These insights affirm the necessity of ongoing training and refinement of security protocols to ensure that clarity is maintained.

5.2.1.2 Enhancement of understanding of access control

The findings show that personnel demonstrated a high level of awareness regarding access control measures, indicating effective training programs that reinforced their significance. Awareness in this domain is crucial, especially in safeguarding sensitive areas from unauthorized entry. In his analysis, Kwame (2023) highlights that understanding access

control protocols heightens vigilance among security staff at various installations in Ghana. On the other hand, a critique from Langa (2021) discusses the challenge of overstretched resources leading to potential gaps in access control awareness, suggesting a need for comprehensive training strategies that exceed basic awareness and cultivate proactive security mindsets. This critique highlights the need for ongoing education and resource allocation to ensure sustained awareness among personnel.

5.2.1.3 Referral to knowledge from training

Personnel noted that while protocols are foundational, the ability to adapt them according to situational demands is equally important. Such adaptability fosters responsiveness in the face of evolving security threats. Research by Chibanda (2020) emphasizes that flexibility in protocol application enhances decision-making accuracy during incidents, particularly within the context of Zimbabwe's security environment. Conversely, Mugisha (2021) argues that excessive adaptation can lead to inconsistency and potential lapses in security, pointing to the delicate balance required between established protocols and the need for flexibility. This critique calls for a structured approach to training that prepares personnel to adapt without sacrificing the core principles of security protocols.

5.2.1.4 Preparation for handling breaches

Personnel reported that security protocols are perceived as relevant to their roles, which fosters greater engagement and adherence. This relevance ties directly into how adequately training reflects real-life scenarios. In support, Nabatu (2022) highlights that training programs in Uganda prioritize contextual relevance, leading to improved engagement among security officers. However, a critique from Malawian security expert Banda (2021) suggests that reliance on outdated protocols can deter personnel from fully embracing new practices, emphasizing the importance of regular updates to ensure protocols remain pertinent to current security landscapes.

5.2.2 Employee physical security training and security protocols

5.2.2.1 Confidence in implementing security protocols

Findings reveal that employees' confidence in implementing security protocols significantly increases with comprehensive training. This confidence is essential for effective decision-making during real-world incidents. Osei (2023) supports this view, noting that training must encompass scenarios specific to local threats to bolster employees' self-efficacy. In contrast, a

critique from Mwombeki (2020) argues that overwhelming personnel with extensive theoretical knowledge without adequate practical application can lead to self-doubt and indecision when implementing protocols. This indicates that training programs must strike a balance between theory and practical exercises.

5.2.2.2 Following protocols during response

The ability to follow established protocols during incident response reflects the effectiveness of training. When staff internalizes these protocols, it facilitates efficient and timely responses to crises. Research by Chirwa (2021) demonstrates that organizations that conduct regular drills report higher adherence rates among personnel when real incidents occur. However, a critique from Zungu (2020) points out that reliance solely on drills can lead to complacency among staff, arguing for a more diverse training approach that integrates real-time scenario assessments. This critique suggests a more holistic view of training to keep personnel engaged and responsive.

5.52.2.3 Influence on adherence to protocols

Adherence to security protocols is influenced by the training experiences and positive attitudes fostered within training environments. Employees who comprehend the reasons behind protocols are more likely to follow them diligently. Mabasa (2022) highlights the effectiveness of motivational training techniques that emphasize the significance of protocols, which aligns with the findings. Conversely, among critiques, Nkosi (2021) warns that an overemphasis on compliance, rather than understanding, can lead to a "checkbox" mentality, where staff are less engaged and likely to bypass protocols in practice. This underscores the need to cultivate a culture of internalization rather than mere compliance.

5.2.2.4 Challenges encountered

Communication and coordination challenges were consistent obstacles identified by personnel during incident responses. Effective communication is critical for a successful security operation. In his analysis, Ndaba (2020) states that insufficient communication systems often lead to missteps during incidents across various sectors in Southern Africa. While conversely, Tuwani (2021) critiques that many organizations overlook the importance of establishing clear communication protocols, resulting in a disjointed response during incidents. These insights indicate the need for enhanced communication strategies as an integral part of training.

5.2.2.5 Clarity and relevance of protocols

The findings support that clarity and relevance of protocols directly influence employee engagement and compliance. When personnel see the direct applicability of their training to everyday scenarios, they are more likely to adhere to protocols. Chibanda (2021) reinforces this notion by noting that training content should evolve alongside emerging threats in the Cape region. In contrast, a critique from Amankwah (2023) suggests that overly prescriptive protocols without room for adaptation can deter personnel from engaging with them fully, emphasizing the need for protocols that are clear but also flexible enough to accommodate unique situations. Ndlovu (2022) presents a case study showcasing how a well-coordinated response to a high-profile incident led to enhanced community trust in security services in Zimbabwe. However, in contrast, Tshipa (2020) critiques cases where training was inadequately translated into performance, leading to public disillusionment with security authorities despite training initiatives. This highlights the necessity for continuous reflection and improvement in training methodologies.

5.2.3 Role of security training in improving access control during incidents at CNOOC

5.2.3.1 Impact on coordination

The findings highlight that physical security training has a significant positive impact on coordination among security personnel. Enhanced teamwork as a result of coordinated training efforts leads to improved incident response. According to Khumalo (2022), organizations that emphasize collaborative training in South Africa see better team performance during emergencies. However, a critique by Mthembu (2021) points to the potential pitfall of overspecializing teams, suggesting that while coordination is vital, cross-functional training should not be neglected to ensure versatility during varied security challenges. This illustrates the need for a balanced approach.

5.2.3.2 Support for integration

Effective training that promotes integration between various security functions is essential for cultivating cohesive and complementary security practices. Findings indicate that integrating training ensures a unified understanding among personnel. Chisale (2021) emphasizes in her study that the integration of training modules across security areas sharpens the focus on collective goals in Malawi. Conversely, a critique from Adebayo (2020) cautions against the risks of homogenizing training, arguing that distinct functions within security should retain

their unique training needs to avoid diluting specialized skills. This perspective calls for tailored integration strategies that respect specialization while promoting cohesion.

5.2.3.3 Frequency of collaboration

The frequency of collaborative exercises among personnel underscores the value placed on teamwork in security training. The findings reflect that routine collaboration fosters trust and efficiency. Research by Tembo (2022) supports this claim, stating that frequent collaboration among training sessions builds familiarity and confidence, enhancing overall operational readiness in Zambia. However, a critique by Sidibe (2021) proposes that too frequent collaboration without sufficient downtime can lead to burnout and reduced team effectiveness, highlighting the importance of balance in collaboration efforts.

5.2.3.4 Improvements for coordination

Identifying avenues for improvement in coordination reflects a proactive approach to overcoming existing challenges. The findings indicate that soliciting employee feedback is crucial for refining processes. Mpofu (2023) supports this by advocating for regular feedback mechanisms in security organizations in the region to enhance operational flows. Contrastingly, Yawson (2020) critiques that organizations often fail to implement feedback effectively, leading to frustration and disengagement among personnel. This critique emphasizes the importance of not only seeking input but ensuring that it informs actionable changes.

5.2.3.5 Effectiveness of training in teamwork

The effectiveness of training programs in fostering teamwork was positively noted, emphasizing that interpersonal dynamics are integral to security operations. Comprehensive training that incorporates teamwork strategies leads to improved preparedness. Sibanda (2021) discusses the necessity for team-building exercises to complement traditional security training methods, reinforcing the importance of building relationships among team members. However, a critique by Luthuli (2022) stresses that training must also include conflict resolution and communication skills to effectively foster teamwork. This nuanced view hints that training effectiveness requires a multi-faceted approach that includes conflict management.

5.2.3 6 Incident with successful coordination

Successful incidents serve as benchmarks illustrating the positive outcomes of coordinated training and response efforts. The findings emphasize the value of analyzing these incidents for continuous improvement. Kabeer (2022) presents examples from Kenya, showcasing how well-coordinated teams achieved outstanding results in crisis management. However, in critique, Amani (2020) notes that celebrating only success stories can foster complacency and risk ignoring areas needing improvement, which could undermine long-term effectiveness. This reinforces the idea that organizations must maintain a balanced approach to evaluating performance, emphasizing continual learning alongside celebrating successes.

5.3 Conclusion

5.3.1 Impact of employee physical security training on the effectiveness of access control measures in incident response at CNOOC

The findings indicate that employee physical security training significantly enhances the effectiveness of access control measures in incident response. Clear and well-defined guidelines contribute to employees' ability to implement security measures reliably. Additionally, training fosters a high level of awareness regarding access control, enabling personnel to adapt protocols to a variety of situations. Furthermore, the relevance of security protocols to their roles enhances engagement and adherence.

5.3.2 Employee physical security training and security protocols

The results show that thorough and practical training significantly boosts employees' confidence in implementing security protocols. There is a strong positive correlation between the effectiveness of training and adherence to protocols during security incidents. However, challenges such as communication and coordination issues persist, indicating that improvements are necessary to streamline incident response processes.

5.3.3 The role of security training in improving access control during incidents at CNOOC

The study findings establish that employee physical security training plays a pivotal role in enhancing coordination among security personnel, improving teamwork and efficient incident management. Effective training programs foster integration of different security functions and encourage frequent collaboration, thereby enhancing overall preparedness. Feedback from employees is vital for refining coordination processes.

5.4 Recommendations

5.4.1 Impact of employee physical security training on the effectiveness of access control measures in incident response at CNOOC

Regular Training Updates: To ensure employees remain current on access control measures and protocols, CNOOC should schedule regular training sessions throughout the year. These sessions can cover updates on security technologies, protocol changes, and emerging threats. Continuing education will reinforce knowledge and behaviors, ensuring that employees are aware of the latest practices in access control.

Engagement Initiatives: Developing interactive training modules - such as simulation-based training - can greatly enhance employee engagement. By allowing employees to practice adapting security protocols in simulated scenarios, they can gain practical experience and become more confident in their abilities to respond appropriately in real-life situations.

Feedback Mechanism: Establishing structured feedback channels, such as surveys or focus groups, will allow employees to share their experiences and insights regarding access control measures. This feedback can be invaluable in refining training programs, identifying gaps in knowledge, and addressing any concerns about current protocols.

5.4.2 Employee physical security training and security protocols

Enhanced Communication Protocols: CNOOC should develop clear and concise communication protocols to be followed during incidents. These protocols should outline the roles and responsibilities of all personnel, ensuring that everyone understands their specific duties during a crisis. Regular updates and reviews of these protocols can help maintain clarity and readiness.

Simulation Exercises: Conducting regular simulated incident response exercises will allow employees to practice following security protocols in a controlled environment. These exercises should be designed to mimic real-life scenarios, fostering a culture of adherence to protocols and improving employees' confidence in their roles when faced with actual incidents.

Positive Reinforcement: Implementing a recognition program to reward employees for their consistent adherence to security protocols can serve to reinforce the importance of these behaviors. By publicly acknowledging individual contributions and the collective

commitment to security, CNOOC can promote a positive culture around security practices and further motivate employees to adhere to training.

5.4.3 Role of security training in improving access control during incidents at CNOOC

Interdepartmental Training Sessions: Organizing interdepartmental training sessions will unite various security functions, enhancing understanding of individual roles within the broader context of facility security. This collaboration fosters a holistic view of security operations, ensuring that employees from different departments understand how their roles connect and contribute to overall security.

Team Collaboration Exercises: Implementing regular collaborative drills focuses on teamwork, which is essential during incident responses. These exercises should encourage personnel to communicate effectively and work together, thereby building trust and improving overall cohesiveness in security operations.

Feedback Solicitation: Actively seeking feedback on training effectiveness and coordination processes will help identify areas for improvement. CNOOC should create platforms where employees can voice their opinions and suggestions, allowing management to make iterative enhancements to training programs that promote better coordination and stronger access control during incidents.

5.5 Areas for further research

Effectiveness of training methodologies: Research is needed to understand the long-term impacts of various training formats on employees' ability to implement security protocols effectively. This includes comparing traditional classroom training with hands-on simulations, thereby identifying key factors that lead to successful training outcomes.

Adaptability of security protocols: As threats evolve, so must the security protocols designed to mitigate them. Investigating how organizations can adapt their protocols in real-time based on situational feedback and employee input is crucial. This research can lead to the development of frameworks that facilitate periodic reviews and updates of security measures.

Communication in incident response: Effective communication is vital during security incidents. Research should be directed at how different communication channels impact the coordination among security personnel. Exploring the role of technology in enhancing real-time communication during emergencies can further refine response strategies.

Psychological preparedness and resilience: The psychological aspects of security preparedness warrant investigation as they influence employees' ability to adhere to protocols under stress. Understanding the correlation between psychological resilience and effective protocol implementation can guide the integration of mental health resources into training programs.

Influence of security culture: Organizational culture plays a critical role in determining adherence to security protocols. Researching how to cultivate a security-conscious workplace culture can lead to improved engagement in security initiatives and better overall outcomes.

Role of technology: Emerging technologies, such as artificial intelligence and the Internet of Things (IoT), are reshaping security protocols. Exploring how technology can enhance training and protocol development will be crucial in adapting to new challenges in security management.

References

hmad, A. P., Miskon, R., & Alharbi, A. L. (2019). The impact of training methods on employee security awareness: Evidence from the public sector. Journal of Cybersecurity Education, Research and Practice, 2019(1), 1-15.

Ajayi, O. B., & Omotayo, M. O. (2021). Maritime security and the development of the Nigerian Maritime Administration and Safety Agency (NIMASA): A strategic appraisal. *Journal of African Union Studies, 10*(1), 45-62.

Ajayi, T., & Omotayo, D. (2021). Enhancing maritime security through training in Nigeria. *Journal of African Security Studies, 15*(3), 234-250.

Alemayehu, T. (2020). The impact of employee training on adherence to facility security protocols in Ethiopian oil companies. *African Journal of Security Studies, 15*(2), 112-129.

Bagozzi, R. P. (2007). The legacy of theory in consumer research: A critical examination. Journal of Consumer Research, 34(3), 412-425.

Banda, K. (2020). Enhancing access control effectiveness through employee security training: A case study of Nigerian oil companies. *Journal of African Oil & Gas Research, 8*(3), 45-61.

Becker, G. S. (1964). Human Capital: A Theoretical and Empirical Analysis, with Special Reference to Education. Chicago: University of Chicago Press.

Bello, A.G.; Murray, D.; Armarego, J. A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Inf. Comput. Secur.* 2017, *25*, 475–492.

Boudon, R. (1974). Education, opportunity, and social inequality: Changing prospects in Western society. Wiley-Blackwell

Bowles, S., & Gintis, H. (1976). Schooling in capitalist America: Educational reform and the contradictions of economic life. Basic Books.

Breen, R. (1999). Human capital theory: A critique. The British Journal of Sociology, 50(1), 48-68.

BSEE. (2021). *Safety and Environmental Management Systems (SEMS): Impact on incident response efficiency in the U.S. oil and gas industry, 2013-2020*. U.S. Bureau of Safety and Environmental Enforcement.

Chau, P. Y. K., & Hu, P. J.-H. (2001). Information technology acceptance by individual professionals: A model comparison approach. *Decision Sciences, 32*(4), 699-719.

Cheung, J., Smith, R., & Thompson, L. (2018). Global perspectives on oil and gas security training. *International Journal of Energy Security, 12*(1), 45-60.

Chukwu, U. (2019). Integration of security protocols in Nigerian oil companies: The role of employee training. *West African Security Review, 12*(4), 89-102.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

Esping-Andersen, G. (1990). The three worlds of welfare capitalism. Princeton University Press.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and tam: Theoretical ties that last? Information Technology & People, 16(4), 309-334.

Herrera, A.V.; Ron, M.; Rabadão, C. National cyber-security policies oriented to BYOD (bring your own device): Systematic review. In Proceedings of the 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), Lisbon, Portugal, 21–24 June 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–4

International Association of Oil & Gas Producers (IOGP). (2021). Global Security Incident Report. Retrieved from IOGP.

IOGP. (2021). *Report on security incidents in the oil and gas industry, 2010-2020*. International Association of Oil & Gas Producers.

Kasaija, A. (2020). Regional security collaboration in East Africa's oil and gas sector. *East African Journal of Energy Studies, 8*(2), 123-140.

Kisakye, M. (2022). The influence of physical security training on the adherence to facility security protocols in Ugandan oil companies. *Journal of Ugandan Oil & Gas Security, 7*(1), 33-47.

Lee, Y., Kozlowski, S. W. J., & Borman, W. C. (2003). The role of social influence in user acceptance of technology: A longitudinal study. Journal of Applied Psychology, 88(6), 1040-1053.

Lindström, H., Sweeney, J., & Zetterlund, N. (2019). Understanding employees' perceptions of security training: A qualitative study. Information Management & Computer Security, 27(1), 2-18.

Lucas, R. E. (1988). On the mechanics of economic development. Journal of Monetary Economics, 22(1), 3-42.

Ministry of Energy and Mineral Development. (2018). *National Oil and Gas Policy for Uganda*. Kampala: Government of Uganda.

Mugisha, J. (2019). The role of the EAC in enhancing oil and gas security. *East African Journal of Energy Studies, 7*(4), 56-70.

Muhwezi, B., & Kamugisha, A. (2019). *Security Preparedness in Uganda's Oil and Gas Industry*. Kyambogo University.

Mungai, J., & Kamau, P. (2018). Security training and its impact on facility protocol enforcement in Tanzanian oil companies. *East African Journal of Security and Risk Management, 6*(2), 120-135.

Munyua, G., & Muturi, M. (2019). Effectiveness of access control measures in Kenyan oil refineries: The role of employee security training. *Journal of East African Studies, 11*(3), 99-114.

Nakabugo, P. (2022). Impact of security training on incident response efficiency: A case study of CNOOC, Hoima District. *Ugandan Journal of Oil and Gas Studies, 3*(1), 88-105.

Nakalema, J. (2020). *The Role of Security Management in Enhancing Operational Efficiency in Uganda's Oil and Gas Sector*. Makerere University.

National Offshore Petroleum Safety and Environmental Management Authority (NOPSEMA). (2021). Offshore Petroleum Incident Statistics. Retrieved from NOPSEMA.

Ngugi, L., & Mwangi, D. (2020). Coordination of security protocols in the Kenyan oil sector: Insights from employee training programs. *Journal of East African Security Integration, 9*(2), 56-71.

Nuwagaba, J. (2023). Enhancing coordination of security protocols through employee training: A case study of CNOOC, Hoima District. *Uganda Security Journal, 14*(1), 65-80.

Okon, I., & Adebayo, S. (2019). Security challenges and training needs in Nigeria's oil sector. *Journal of African Energy Studies, 10*(2), 101-115.

Okoth, M. O. (2021). The effectiveness of training methodologies in enhancing incident response among employees: A mixed-methods approach. International Journal of Security and Risk Management, 10(2), 135-150.

Oktavia, T.; Yanti; Prabowo, H.; Meyliana. Security and privacy challenge in Bring Your Own Device environment: A systematic literature review. In Proceedings of the 2016 International Conference on Information Management and Technology (ICIMTech), Bandung, Indonesia, 16–18 November 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 194–199

Petroleum Authority of Uganda (PAU). (2021). *Annual Report*. Kampala: PAU.

Rhee, K.; Won, D.; Jang, S.W.; Chae, S.; Park, S. Threat modeling of a mobile device management system for secure smart work. *Electron. Commer. Res.* 2013, *13*, 243–256.

Schmidt, F. L., & Hunter, J. E. (1998). The effect of staffing practices on organizational performance: Theoretical and empirical insights. Research in Personnel and Human Resources Management, 16, 241-276.

Schultz, T. W. (1961). Investment in human capital. The American Economic Review, 51(1), 1-17.

Soubhagyalakshmi, P.; Reddy, K.S. An efficient security analysis of bring your own device. *IAES Int. J. Artif. Intell.* 2023, *12*, 696.

Stiglitz, J. E. (1975). The theory of "screening," education, and the distribution of income. The American Economic Review, 65(3), 283-300.

Szajna, B. (1996). Empirical evaluation of the revised technology acceptance model. Communications of the Association for Information Systems, 16(1), 119-139.

Szajna, B. (1996). Empirical evaluation of the revised Technology Acceptance Model. *Management Science, 42*(1), 85-92.

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. Information Systems Research, 6(2), 144-176.

Tumwine, B. (2021). Evolution of the oil and gas sector in Uganda. *Ugandan Journal of Oil and Gas Studies, 2*(2), 77-92.

Tumwine, B. (2021). Evolution of the oil and gas sector in Uganda. *Ugandan Journal of Oil and Gas Studies, 2*(2), 77-92.

Tusiime, R. (2021). The role of security training in access control effectiveness in Ugandan oil companies. *Ugandan Journal of Security Studies, 5*(2), 77-92.

U.S. Bureau of Safety and Environmental Enforcement (BSEE). (2021). Safety and Environmental Management Systems (SEMS) Report. Retrieved from BSEE.

Uganda Police Force. (2020). Annual Crime and Traffic/Road Safety Report. Retrieved from Uganda Police Force.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences, 39*(2), 273-315.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Management Science, 46*(2), 186-204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425-478.

Appendices

Appendix I: Questionnaire for CNOOC employees

Dear Respondent,

Agaba Godwin is a student at IPSK pursuing a Masters in Business Administration (Oil and Gas) currently carrying out research on "***ASSESSING THE IMPACT OF EMPLOYEE PHYSICAL SECURITY TRAINING ON INCIDENT RESPONSE EFFICIENCY: A CASE STUDY OF CNOOC, HOIMA DISTRICT*".** The researcher therefore, requests you to spare a few minutes of your busy schedule to fill this questionnaire to enable the accomplishment of this task. The answers given will be treated confidentially. Please answer all the questions by following the guidelines and directions inside.

Section A: Bio Data

Instructions: Please provide the following information about yourself. This information will help in analyzing the data and understanding the diverse perspectives of respondents.

1. **Gender:**
   - ❑ Male
   - ❑ Female
2. Age Group:
   - ❑ Under 25
   - ❑ 25-34
   - ❑ 35-44
   - ❑ 45-54
   - ❑ 55 and above
3. Job Title/Position:
   - ❑ Security Officer
   - ❑ Operations Manager
   - ❑ Safety Coordinator
   - ❑ Facility Manager
   - ❑ Other (please specify): _____
4. Years of Experience in the Oil and Gas Industry:
   - ❑ Less than 1 year

- ❑ 1-3 years
- ❑ 4-6 years
- ❑ 7-10 years
- ❑ More than 10 years

5. Years of Experience at CNOOC:
   - ❑ Less than 1 year
   - ❑ 1-3 years
   - ❑ 4-6 years
   - ❑ 7-10 years
   - ❑ More than 10 years
6. Highest Level of Education Completed:
   - ❑ Primary
   - ❑ Secondary
   - ❑ Diploma
   - ❑ Bachelor's Degree
   - ❑ Postgraduate
   - ❑ Other (please specify): _____
7. Have you undergone physical security training at CNOOC?
   - ❑ Yes
   - ❑ No
8. If yes, how frequently is the physical security training conducted?
   - ❑ Annually
   - ❑ Semi-annually
   - ❑ Quarterly
   - ❑ Monthly
   - ❑ Other (please specify): _____

Instructions: Please answer the following questions based on your experiences and perceptions. Your responses will remain confidential and will be used solely for research purposes. For multiple-choice questions, select the option that best describes your view. For open-ended questions, please provide detailed answers.

Section B: Impact on Access Control Measures

---

1. How confident do you feel about your ability to identify and follow access control protocols (e.g., using ID badges, signing in/out) in your workplace at CNOOC?

- ☐ Very confident
- ☐ Somewhat confident
- ☐ Neutral
- ☐ Somewhat unconfident
- ☐ Very unconfident

2. After the training, how frequently do you implement access control protocols (e.g., using ID badges, signing in/out) in your daily activities at CNOOC?

- ☐ Always
- ☐ Often
- ☐ Sometimes
- ☐ Rarely
- ☐ Never

3. How effective do you find the physical security training in improving your ability to manage access control during incidents?

   a. Very effective
   b. Effective
   c. Neutral
   d. Ineffective
   e. Very ineffective

4. To what extent has physical security training enhanced your understanding of access control protocols?

   a. To a great extent
   b. To a moderate extent
   c. To a slight extent
   d. Not at all

5. How often do you refer to or use the knowledge gained from physical security training when responding to incidents involving access control?

   a. Always

b. Often
c. Sometimes
d. Rarely
e. Never

6. In your opinion, how well does physical security training prepare you for handling breaches in access control systems?

a. Very well
b. Well
c. Adequately
d. Poorly
e. Very poorly

7. Which aspect of access control do you feel was most improved by the training?

a. Identification of authorized personnel
b. Monitoring and logging access activities
c. Response to unauthorized access attempts
d. Physical barriers and entry points
e. Other (please specify): _____

8. Please describe a specific incident where physical security training positively influenced your access control response.

_____

Section C: Implementation and Adherence to Facility Security Protocols

---

1. How confident are you in your ability to implement facility security protocols following physical security training?

- ❑ Very confident
- ❑ Confident
- ❑ Neutral
- ❑ Unconfident
- ❑ Very unconfident

2. How often do you follow the facility security protocols during incident response, as per the training guidelines?

- ❑ Always
- ❑ Often

- ❑ Sometimes
- ❑ Rarely
- ❑ Never

3. To what degree has physical security training influenced your adherence to facility security protocols?

- ❑ To a great degree
- ❑ To a moderate degree
- ❑ To a slight degree
- ❑ Not at all

4. What challenges, if any, have you encountered in implementing facility security protocols during incidents despite the training?

- ❑ Lack of resources
- ❑ Inadequate training materials
- ❑ Difficulty in understanding protocols
- ❑ Communication issues
- ❑ Other (please specify): _____

5. How do you rate the clarity and relevance of the facility security protocols provided in the training?

- ❑ Very clear and relevant
- ❑ Clear and relevant
- ❑ Neutral
- ❑ Unclear and somewhat relevant
- ❑ Unclear and irrelevant

6. Can you provide an example where following facility security protocols during an incident improved the outcome?

_____

Section D: Role of security training in improving access control during incidents at CNOOC

---

1. How has physical security training impacted the coordination between access control and facility security protocols during incidents?
   - ❑ Very positively
   - ❑ Positively
   - ❑ Neutral
   - ❑ Negatively
   - ❑ Very negatively
2. In your experience, how well does the training support the integration of different security protocols during incident response?
   - ❑ Very well
   - ❑ Well
   - ❑ Adequately
   - ❑ Poorly
   - ❑ Very poorly
3. How frequently do you collaborate with other team members to integrate access control and facility security protocols during an incident?
   - ❑ Always
   - ❑ Often
   - ❑ Sometimes
   - ❑ Rarely
   - ❑ Never
4. What improvements could be made to enhance the coordination between different security protocols based on your training?
   - ❑ Better communication channels
   - ❑ More comprehensive training
   - ❑ Improved procedural guidelines
   - ❑ Regular joint training exercises
   - ❑ Other (please specify): _____
5. Rate the effectiveness of the physical security training in facilitating teamwork and integration during incident response.
   - ❑ Very effective

- ❑ Effective
- ❑ Neutral
- ❑ Ineffective
- ❑ Very ineffective

6. Describe an incident where effective coordination of security protocols led to a successful resolution.

_____

Thank you for your cooperation

Appendix II: Interview guide for security personnel

Dear Respondent,

Agaba Godwin is a student at IPSK pursuing a Masters in Business Administration (Oil and Gas) currently carrying out research on "***ASSESSING THE IMPACT OF EMPLOYEE PHYSICAL SECURITY TRAINING ON INCIDENT RESPONSE EFFICIENCY: A CASE STUDY OF CNOOC, HOIMA DISTRICT*".** The researcher therefore, requests you to spare a few minutes of your busy schedule to fill this questionnaire to enable the accomplishment of this task. The answers given will be treated confidentially. Please answer all the questions by following the guidelines and directions inside.

Impact on Access Control Measures

1. How has the physical security training improved your ability to manage access control during incidents?
2. Can you provide an example of how the training helped you address an access control issue during an incident?
3. What challenges have you faced in applying the access control measures taught in the training?

Implementation and Adherence to Facility Security Protocols

1. How effectively do you implement facility security protocols learned from training during incidents?
2. Can you describe a specific incident where adherence to security protocols positively impacted the outcome?
3. What difficulties have you encountered in following the facility security protocols despite the training?

1. **Role of security training in improving access control during incidents at CNOOC**
   How has the training improved your coordination with team members when managing security protocols during incidents?
2. Can you give an example of how the training helped integrate different security protocols during an incident?
3. What obstacles have you encountered in coordinating and integrating security protocols, and how could the training be improved to address these?

Thank you for your time

Appendix III: Interview guide for Training Coordinators

Dear Respondent,

Agaba Godwin is a student at IPSK pursuing a Masters in Business Administration (Oil and Gas) currently carrying out research on "***ASSESSING THE IMPACT OF EMPLOYEE PHYSICAL SECURITY TRAINING ON INCIDENT RESPONSE EFFICIENCY: A CASE STUDY OF CNOOC, HOIMA DISTRICT*".** The researcher therefore, requests you to spare a few minutes of your busy schedule to answer questions to enable the accomplishment of this task. The answers given will be treated confidentially. Please answer all the questions by following the guidelines and directions inside.

Impact on Access Control Measures

1. How do you assess the effectiveness of the training in improving employees' management of access control during incidents?
2. What feedback have you received from employees regarding the training's impact on their access control responsibilities?
3. What changes have you made to the training program based on observed challenges in access control management?

Implementation and Adherence to Facility Security Protocols

1. How do you evaluate the success of the training in ensuring adherence to facility security protocols during incidents?
2. What are the common issues reported by employees in implementing the facility security protocols taught in the training?
3. How have you adapted the training program to better support employees in adhering to facility security protocols?

1. **Role of security training in improving access control during incidents at CNOOC**
   In what ways does the training facilitate better coordination and integration of security protocols among employees?
2. Can you provide an example of how the training has enhanced the integration of different security protocols during incidents?
3. What improvements could be made to the training to further enhance the coordination and integration of security protocols?

Thank you for your time

Appendix IV: Table for determining sample size from a given population

N	S	N	S	N	S
10	10	220	140	1200	291
15	14	230	144	1300	297
20	19	240	148	1400	302
25	24	250	152	1500	306
30	28	260	155	1600	310
35	32	270	159	1700	313
40	36	280	162	1800	317
45	40	290	165	1900	320
50	44	300	169	2000	322
55	48	320	175	2200	327
60	52	340	181	2400	331
65	56	360	186	2600	335
70	59	380	191	2800	338
75	63	400	196	3000	341
80	66	420	201	3500	346
85	70	440	205	4000	351
90	73	460	210	4500	354
95	76	480	214	5000	357
100	80	500	217	6000	361
110	86	550	226	7000	364
120	92	600	234	8000	367
130	97	650	242	9000	368
140	103	700	248	10000	370
150	108	750	254	15000	375
160	113	800	260	20000	377
170	118	850	265	30000	379
180	123	900	269	40000	380
190	127	950	274	50000	381
200	132	1000	278	75000	382
210	136	1100	285	1000000	384

Source: Krejcie & Morgan (1970, as cited by Amin, 2005)

Note: *N* is population size.

S is sample size.