INTEGRATED SECURITY SOLUTIONS IN MANUFACTURING INDUSTRIES AND ITS IMPACT TO LOSS PREVENTION IN NAIROBI CITY COUNTY, KENYA

Amos Muiruri Mburu.
Post-Graduate Students – Master of Security Management and Police Studies, Kenyatta University, Kenya.

ABSTRACT

The manufacturing sector has always been a cornerstone of economic development, particularly in rapidly urbanizing regions like Nairobi, Kenya. As industrial activities expand, so do the associated risks, including theft, vandalism, and operational losses. Nairobi's industrial area, in particular, has witnessed significant challenges related to security, impacting the overall efficiency and profitability of manufacturing firms. Loss prevention in this sector has grown in importance, necessitating the adoption of comprehensive security measures that are both proactive and reactive. Integrated security solutions, which encompass a combination of personnel, technology, and procedures, have emerged as an essential strategy for manufacturers aiming to safeguard their assets. The study objectives were; to assess the existing security frameworks utilized by manufacturing firms in Kenya, identifying both technological and human resource components and to identify key challenges in implementing integrated security solutions. The study was guided by Routine activity theory which was developed by Lawrence E. Cohen and Marcus Felson (1979). The study adopted an explanatory research design. The target population of the study comprised manufacturing firms operating within Nairobi's Industrial Area. According to the Nairobi County Government (2021), there are approximately 150 registered manufacturing firms in this area. A stratified random sampling technique was used to ensure that the sample was representative of different types of manufacturing firms within the Industrial Area. The population was divided into strata based on the size of the firm (small, medium, and large). A sample size of 50 firms was selected. This sample size was determined based on Yamane's (1967) formula. The study relied on secondary data as the primary research instrument. Data analysis was conducted using both descriptive and inferential statistical methods. The study revealed that most manufacturing firms in Nairobi's Industrial Area employed a combination of technological and human resource components in their security frameworks. Descriptive statistics indicated that 80% of the firms used surveillance technologies, such as CCTV cameras, as their primary security tool. The findings from inferential statistics showed a positive correlation ($r = 0.72$, $p < 0.05$) between the use of integrated security systems (technology and human resources) and loss prevention, indicating that firms with more comprehensive security frameworks experienced fewer security breaches. The study also identified several key challenges faced by manufacturing firms when implementing integrated security solutions. Additionally, 45% of the respondents mentioned difficulties in keeping up with technological advancements, as systems often became outdated quickly, requiring frequent upgrades. The study concluded that the integration of technological and human resource components plays a pivotal role in enhancing loss prevention. Manufacturing firms that implemented advanced security systems such as surveillance cameras, biometric access controls, and alarm systems, in conjunction with trained security personnel, experienced fewer security breaches and significant reductions in losses caused by

theft, vandalism, and operational disruptions. Manufacturing firms, especially SMEs, should explore cost-effective security technologies that offer scalable solutions. Governments and industry bodies can assist by providing incentives, subsidies, or tax reliefs to lower the initial costs of implementing advanced security systems, enabling more firms to adopt these technologies. The study recommended that manufacturing firms should invest in regular training programs to enhance the skills of security personnel responsible for managing and operating integrated security systems. Firms must prioritize regular upgrades and maintenance of their security systems to ensure that they remain effective and up to date.

INTRODUCTION

Manufacturing firms have become a major target of theft, vandalism, management-labor-related disputes, property damage, equipment and product tampering, and litigation (Awino & Olatunji, 2021). And as products and processes continue to be developed, manufactured, and distributed, an extremely professional level of security planning, prevention and protection is required. Security starts at the perimeter to prevent unauthorized entry. From detecting suspicious activity at a chemical plant or unlawful entry at an airline hangar, intrusion detection and perimeter security help proactively identify threats before they escalate.

Safeguarding both tangible and intangible assets has become paramount as industrial operations continue to face evolving threats, including theft, sabotage, and operational disruptions. Integrated security solutions, which combine technological systems, physical security measures, and personnel management, have emerged as essential tools in mitigating risks within these sectors. Manufacturing industries, particularly in urban areas such as Nairobi's Industrial Area, have increasingly adopted these integrated systems to bolster their loss prevention efforts. The need to ensure the protection of manufacturing processes, infrastructure, and sensitive data has heightened as the region experiences significant industrial growth. Nairobi's Industrial Area, being a hub for various large-scale and small-scale manufacturers, presents unique challenges for security management due to its diverse industrial activities and high population density, which increases the likelihood of security threats (Kamau, 2021).

Loss prevention in manufacturing involves reducing the frequency and severity of losses that can negatively impact productivity, profitability, and asset management. Traditional security approaches, such as standalone physical barriers and manual surveillance, have proven inadequate in dealing with modern-day threats. This has driven manufacturers in Industrial Area, Nairobi, to integrate various security measures such as surveillance technologies, access control systems, and alarm systems into a cohesive framework (Karanja & Mwangi, 2019). These integrated security solutions combine information from multiple sources cameras, sensors, employee badges and provide centralized control for quicker and more efficient responses to security breaches. This shift toward an integrated approach is largely driven by the increasing sophistication of security threats and the need for more cost-effective, scalable, and adaptive security measures (Ogolla & Njeri, 2020).

Moreover, the adoption of integrated security solutions has shown promising results in minimizing losses, particularly in industries where theft, unauthorized access, and operational downtimes are major concerns. For example, industries within Nairobi's Industrial Area have reported improved incident response times, better coordination between security teams, and a significant reduction in losses related to theft and damage since adopting integrated systems (Mwangi et al., 2020). These solutions not only enhance security but also contribute to operational efficiency by automating routine security tasks and allowing management to focus on core business activities. In this context, the role of integrated security in loss prevention is

critical as manufacturers continue to balance cost management with the need for robust security measures.

The integration of security technologies such as CCTV surveillance, access control systems, and alarm systems has become increasingly prevalent (Gikonyo, 2022). These technologies, when harmonized with human resources and operational protocols, create a security framework that is not only robust but also adaptable to the unique challenges faced by the industrial sector. The need for such comprehensive approaches has been underscored by the rising crime rates in urban industrial areas and the financial implications that accompany these losses (Odhiambo, 2020).

Despite the clear benefits, challenges remain in the implementation of these integrated security solutions. For one, the high initial costs associated with setting up these systems can deter some manufacturers from adopting them fully. Additionally, there is a growing need for security personnel to be trained in the use of advanced security technologies, as the effectiveness of integrated solutions largely depends on human oversight and decision-making (Muthoni & Nyabuto, 2021). Nevertheless, as security threats in Nairobi's Industrial Area become more sophisticated, the investment in integrated security solutions is viewed as a necessary measure for long-term loss prevention.

Statement of the Problem

Manufacturing industries in Nairobi's Industrial Area have been facing persistent challenges related to security breaches, including theft, vandalism, unauthorized access, and sabotage, which result in significant financial losses and operational inefficiencies. Traditional security measures, such as manual guards and isolated alarm systems, have proved inadequate in addressing the growing complexity and sophistication of security threats in the industrial sector (Kamau, 2021). As a result, manufacturing firms are increasingly adopting integrated security solutions that combine physical, technological, and personnel-based measures to enhance loss prevention and ensure the continuity of business operations.

Despite the adoption of integrated security solutions in some industries, many manufacturers in Nairobi's Industrial Area continue to suffer substantial losses due to security failures. Research has shown that incidents of theft, both internal and external, as well as sabotage, remain prevalent, causing a significant impact on profitability and supply chain reliability (Mwangi et al., 2020). This suggests that either the integrated security solutions implemented are not comprehensive enough, or there are gaps in their application and management. The complexity of managing security systems that include surveillance cameras, biometric access control, and alarm systems requires technical expertise and continuous monitoring, which may not be fully available or adequately utilized by these industries (Muthoni & Nyabuto, 2021). Furthermore, the integration of technology with human oversight is essential for detecting and responding to threats effectively, yet many firms report challenges in aligning these aspects of security management.

The problem is exacerbated by the lack of specific research focusing on the impact of integrated security solutions on loss prevention within Nairobi's manufacturing sector. While there is general literature on security systems in industrial settings, there is a gap in understanding how integrated security solutions have been implemented and whether they have significantly contributed to reducing losses in Nairobi's Industrial Area (Ogolla & Njeri, 2020). This study sought to fill this gap by examining the effectiveness of integrated security solutions in preventing losses in the manufacturing industries located in Industrial Area, Nairobi City County, Kenya.

Objectives of the Study

The study was guided by the following research objectives;
i.   To assess the existing security frameworks utilized by manufacturing firms in Kenya, identifying both technological and human resource components.
ii.   To identify key challenges in implementing integrated security solutions.

Significance of the Study

Firstly, the findings of this study provided valuable findings to manufacturing industry managers and decision-makers in Industrial Area, Nairobi, Kenya. Through understanding the effectiveness of integrated security solutions in preventing losses, they would make informed decisions on investing in appropriate security measures to safeguard their assets and enhance operational efficiency. This knowledge could help them optimize resource allocation and prioritize security initiatives to mitigate potential risks.

Secondly, the study's implications extend to the employees and workers within the manufacturing industries in Industrial Area. Enhanced security measures not only protect the physical assets of the company but also contribute to creating a safer work environment. This is enhanced by reducing the risk of theft, vandalism, or other criminal activities, employees will focus on their tasks without fear or disruption, leading to improved productivity and job satisfaction.

LITERATURE REVIEW

Kamau (2021) conducted a study examining the effectiveness of integrated security systems in manufacturing industries located in Nairobi's Industrial Area. The study employed a descriptive research design to investigate how different components of security systems, such as surveillance cameras, biometric access control, and security personnel, contributed to the reduction of theft and operational disruptions. The target population consisted of 50 manufacturing firms within Nairobi's Industrial Area, with the respondents including security managers and operational heads. Data was collected through structured questionnaires, and the findings revealed that firms that implemented comprehensive integrated security solutions experienced a 40% reduction in security breaches over a three-year period. The study also found that real-time monitoring through surveillance technologies was a key factor in deterring potential criminal activities.

Similarly, Karanja and Mwangi (2019) explored the role of technological solutions in loss prevention across Kenya's manufacturing sector. Using a cross-sectional survey design, the researchers targeted 60 manufacturing firms in Nairobi, Mombasa, and Kisumu. The study aimed to assess the impact of combining physical and technological security measures on minimizing internal theft and external attacks. Questionnaires were administered to security personnel and senior managers. The findings indicated that firms that adopted a mix of access control technologies, such as biometric systems and surveillance cameras, in addition to traditional security personnel, reduced internal theft by 35%. However, the study highlighted that the success of these security solutions depended on regular system upgrades and employee training, which were sometimes lacking in smaller manufacturing firms.

Mwangi, Maina, and Waweru (2020) conducted an empirical study on the influence of security technologies on loss prevention in Kenya's manufacturing sector. They used a mixed-methods research design, combining qualitative interviews and quantitative surveys to gather comprehensive data. The target population comprised 45 manufacturing industries in Nairobi's Industrial Area. The researchers specifically focused on firms that had adopted integrated security solutions within the last five years. The findings showed that 90% of the firms that had invested in advanced security systems, such as integrated surveillance and intrusion detection systems, experienced a significant reduction in both external theft and workplace accidents. The study further found that these security solutions improved operational efficiency by automating routine security tasks, which allowed firms to allocate resources more efficiently. However, the study pointed out that the high cost of implementing these systems posed a challenge for some firms.

Theoretical Framework

The study was guided by Routine activity theory which was developed by Lawrence E. Cohen and Marcus Felson (1979). The theory posits that criminal activities are likely to occur when three elements converge: A motivated offender, a suitable target, and the absence of a capable guardian (Cohen & Felson, 1979). In the context of manufacturing industries, especially in Nairobi's Industrial Area, these elements are frequently present due to the high concentration of valuable assets, such as machinery, raw materials, and finished products, making them attractive targets for theft, vandalism, or sabotage. The theory suggests that crime is deterred by increasing guardianship and reducing opportunities for offenders through systematic monitoring and control (Clarke, 1995).

Integrated security solutions align directly with Routine Activity Theory by enhancing the role of guardianship through technology and personnel, thus limiting opportunities for crime. These systems incorporate surveillance cameras, access control mechanisms, alarms, and security personnel into a cohesive framework that constantly monitors potential offenders, protects valuable targets, and responds swiftly to any threats. In manufacturing industries, where routine operations involve the movement of goods, raw materials, and employees, integrated security solutions play a key role in minimizing opportunities for crime by creating an omnipresent security layer. For instance, the use of access control systems ensures that only authorized

personnel can enter restricted areas, thus reducing the chance of internal theft or sabotage (Ogolla & Njeri, 2020).

Furthermore, by integrating advanced surveillance and monitoring technologies, these systems act as a form of continuous guardianship, reducing the likelihood of crime even in the absence of physical security personnel. According to Mwangi et al. (2020), many manufacturing industries in Nairobi's Industrial Area have reported a significant decrease in security incidents following the installation of integrated security systems. These systems not only detect and deter potential offenders but also ensure real-time incident reporting, allowing for a quick response, which is essential for preventing or minimizing losses.

However, the effectiveness of integrated security solutions, in line with Routine Activity Theory, depends on the efficient management and maintenance of these systems. Muthoni and Nyabuto (2021) argue that even with advanced technological solutions, there must be human oversight to interpret the data provided by these systems and take appropriate action. This combination of technology and human intervention ensures that the 'capable guardian' component of Routine Activity Theory is always present, thereby minimizing the risk of crime in the manufacturing sector. Without these integrated systems, industries in Nairobi's Industrial Area would remain vulnerable, as offenders could easily exploit gaps in traditional security methods, such as unmanned entry points or blind spots in surveillance (Kamau, 2021).

RESEARCH METHODOLOGY

Research Design
The study adopted an explanatory research design. This design is suitable for examining cause-and-effect relationships, making it ideal for assessing how integrated security solutions influence loss prevention within manufacturing industries (Saunders, Lewis, & Thornhill, 2016). Explanatory research helps in establishing the relationship between variables by explaining the underlying mechanisms of these relationships (Cooper & Schindler, 2014). In this case, the study aimed to explore how various security measures, including surveillance systems, access control, and alarm systems, collectively contribute to reducing security breaches and preventing losses in manufacturing firms.

Target Population
The target population of the study comprised manufacturing firms operating within Nairobi's Industrial Area. The region is a major hub for industrial activity in Kenya, hosting numerous firms across various sectors, including food processing, chemicals, textiles, and machinery. According to the Nairobi County Government (2021), there are approximately 150 registered manufacturing firms in this area. The study focused specifically on firms that have implemented integrated security systems, which narrowed down the target population to around 100 firms. The respondents included security managers, operations managers, and other relevant personnel responsible for overseeing security protocols within these organizations.

Sampling Techniques and Sample Size

A stratified random sampling technique was used to ensure that the sample was representative of different types of manufacturing firms within the Industrial Area. Stratified random sampling is appropriate when the population consists of subgroups that may differ significantly, allowing the researcher to ensure that each group is proportionately represented in the sample (Bryman & Bell, 2015). The population was divided into strata based on the size of the firm (small, medium, and large). A sample size of 50 firms was selected, representing 50% of the firms with integrated security systems. This sample size was determined based on Yamane's (1967) formula, which is used to calculate the required sample size from a known population while considering an acceptable margin of error.

Research Instruments

The study relied on secondary data as the primary research instrument. Secondary data was collected from various sources, including company security reports, loss prevention records, and operational efficiency reports from the firms under study. Additionally, industry reports, journals, and previous studies related to integrated security systems were reviewed to provide context and support the data analysis. Secondary data was particularly useful in this study because it provided existing, quantifiable information on the relationship between integrated security solutions and loss prevention, helping to assess the overall effectiveness of these systems.

Data Analysis

Data analysis was conducted using both descriptive and inferential statistical methods. Descriptive statistics, such as means, frequencies, and percentages, were used to summarize the data and present an overview of the impact of integrated security solutions on loss prevention (Kothari, 2004). Inferential statistics, specifically regression analysis, was employed to establish the relationship between the independent variable (integrated security solutions) and the dependent variable (loss prevention). Regression analysis helps to quantify the strength and direction of the relationship between these variables (Field, 2018). Statistical software, SPSS, was used for data analysis, and the results were presented in the form of tables, charts, and graphs to ensure clarity and facilitate interpretation.

FINDINGS AND DISCUSSIONS

Existing security frameworks utilized by manufacturing firms in Kenya

The study revealed that most manufacturing firms in Nairobi's Industrial Area employed a combination of technological and human resource components in their security frameworks. Descriptive statistics indicated that 80% of the firms used surveillance technologies, such as CCTV cameras, as their primary security tool. Additionally, 60% of the firms had implemented biometric access control systems to regulate employee movement and prevent unauthorized access to restricted areas. These technological solutions were complemented by physical security measures, such as alarm systems (utilized by 55% of the firms) and fencing with controlled entry points (70% of the firms).

In terms of human resources, 90% of the firms employed security personnel to oversee the technological components and manage day-to-day security operations. The integration of human oversight with technology was viewed as a critical factor in enhancing the effectiveness of security systems. For instance, security personnel were responsible for monitoring CCTV feeds, managing access control systems, and responding to alarms. The findings from inferential statistics showed a positive correlation ($r = 0.72$, $p < 0.05$) between the use of integrated security systems (technology and human resources) and loss prevention, indicating that firms with more comprehensive security frameworks experienced fewer security breaches. Consistent with the literature, the use of advanced technologies such as surveillance cameras, biometric access control, and alarm systems was found to have a significant positive impact on loss prevention (Kamau, 2021). However, the study also highlighted the crucial role of security personnel in managing these technologies, aligning with Karanja and Mwangi's (2019) assertion that human oversight is essential for the effective functioning of security systems.

Key challenges in implementing integrated security solutions

The study also identified several key challenges faced by manufacturing firms when implementing integrated security solutions. The descriptive analysis revealed that 65% of the firms struggled with the high cost of installation and maintenance of advanced security technologies. Firms indicated that initial setup costs for comprehensive systems, including surveillance cameras, access control, and alarm systems, were prohibitively expensive for small and medium-sized enterprises (SMEs). Additionally, 45% of the respondents mentioned difficulties in keeping up with technological advancements, as systems often became outdated quickly, requiring frequent upgrades.

Another significant challenge was the lack of skilled personnel to manage integrated security systems, which was reported by 40% of the firms. Many organizations noted that while they had invested in advanced technologies, they lacked adequately trained staff to operate and maintain these systems effectively. This led to inefficient use of security technologies, reducing their potential impact on loss prevention.

Further, the inferential analysis indicated that there was a negative correlation ($r = -0.54$, $p < 0.05$) between the lack of skilled personnel and the effectiveness of security solutions, meaning that firms with insufficiently trained staff experienced higher rates of security breaches. The findings suggested that while technology was an important component of security frameworks, the human element was equally critical for the successful implementation and operation of these systems.

Finally, 25% of the firms reported challenges related to employee resistance to the implementation of new security technologies, especially biometric access control systems. Employees often perceived these systems as invasive and a violation of privacy, leading to compliance issues. The study found that overcoming such resistance required continuous training and engagement with employees to explain the benefits of the systems for overall security and organizational efficiency. The challenges identified in the study, including the high costs of technology and the lack of skilled personnel, mirror the findings of Mwangi,

Maina, and Waweru (2020), who noted that small and medium-sized enterprises face significant financial and operational barriers in adopting integrated security solutions. The correlation between a lack of trained personnel and higher security breaches points to the need for ongoing training and capacity-building initiatives to ensure that firms can maximize the potential of their security investments.

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

The study concluded that the integration of technological and human resource components plays a pivotal role in enhancing loss prevention. Manufacturing firms that implemented advanced security systems such as surveillance cameras, biometric access controls, and alarm systems, in conjunction with trained security personnel, experienced fewer security breaches and significant reductions in losses caused by theft, vandalism, and operational disruptions. The positive correlation found between integrated security solutions and improved loss prevention highlights the critical importance of combining both technology and human oversight to optimize security. However, the research also identified several key challenges that hindered the effective implementation of integrated security solutions. These included the high costs associated with acquiring and maintaining security technologies, the rapid obsolescence of these systems, a shortage of skilled personnel, and resistance from employees toward certain security measures.

Recommendations

The study recommended that;

i. Manufacturing industries to exploit use of perimeter intruder detection systems, audio interventions well supported by integrated security operation center-ISOC

ii. Utilizing enhanced CCTV analytics with artificial intelligence allows for the proactive detection of potential risks and suspicious behavior patterns. This technology aids in ensuring the secure dispatch of finished products by monitoring fleet activity and automating dispatch systems. Additionally, the double-checking of merchandise before dispatch helps to prevent errors and inaccuracies.

iii. Security personnel should be trained on loss prevention measures, thorough frisking procedures, and conducting frequent patrols to ensure the safety and security of the delivery process. End-to-end verification of dispatch and delivery documentations is also conducted to confirm the accurate transfer of goods. Additionally, measures are put in place to control and minimize merchandise damages during transit.

iv. Introduction of cage systems to tinny size merchandise, ensure the cages within the ware house are under key and lock, well issuance and documentations.

v. Manufacturing firms, especially SMEs, should explore cost-effective security technologies that offer scalable solutions. Governments and industry bodies can assist by providing incentives, subsidies, or tax reliefs to lower the initial costs of implementing advanced security systems, enabling more firms to adopt these technologies.

vi.   Firms should invest in regular training programs to enhance the skills of security personnel responsible for managing and operating integrated security systems. This training should cover not only the use of the technologies but also how to effectively respond to security incidents. Collaboration with security experts and training institutions could help bridge the skills gap.

vii.   To reduce employee resistance to new security technologies, firms should engage workers by clearly communicating the benefits of these systems in enhancing safety and operational efficiency. Conducting awareness campaigns and involving employees in the decision-making process related to security measures can improve compliance and foster a security-conscious culture within the organization.

viii.   Firms must prioritize regular upgrades and maintenance of their security systems to ensure that they remain effective and up to date. This could include working with vendors to implement cost-efficient maintenance contracts or choosing security technologies with flexible, upgradeable features that can adapt to emerging threats.

REFERENCES

Awino, R., & Olatunji, O. (2021). Integrated Security Solutions: A Systematic Review of Factors Influencing Implementation in Manufacturing Industries. *Journal of Security Studies, 15*(2), 145-163.

Bryman, A., & Bell, E. (2015). *Business Research Methods* (4th ed.). Oxford University Press.

Clarke, R. V. (1995). *Situational Crime Prevention: Successful Case Studies (2nd ed.).* Harrow and Heston.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608.

Cooper, D. R., & Schindler, P. S. (2014). *Business Research Methods* (12th ed.). McGraw-Hill.

Field, A. (2018). *Discovering Statistics Using IBM SPSS Statistics* (5th ed.). SAGE Publications.

Gikonyo, P. (2022). The Role of Technology in Enhancing Security for Manufacturing Firms in Nairobi. *International Journal of Industrial Management, 12*(3), 230-245.

Kamau, J. (2021). Challenges of industrial security management in Nairobi's industrial sector. *Journal of Security Studies, 12*(3), 45-60.

Kamau, J. (2021). Challenges of industrial security management in Nairobi's industrial sector. *Journal of Security Studies, 12*(3), 45-60.

Karanja, P., & Mwangi, D. (2019). Technological solutions for loss prevention in Kenya's manufacturing industries. *African Journal of Industrial Research, 8*(2), 78-92.

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques* (2nd ed.). New Age International Publishers.

Muthoni, W., & Nyabuto, G. (2021). Human factors in the implementation of integrated security systems in manufacturing industries. *Journal of Industrial Security, 5*(4), 125-138.

Muthoni, W., & Nyabuto, G. (2021). Human factors in the implementation of integrated security systems in manufacturing industries. *Journal of Industrial Security, 5*(4), 125-138.

Muthoni, W., & Nyabuto, G. (2021). Human factors in the implementation of integrated security systems in manufacturing industries. *Journal of Industrial Security, 5*(4), 125-138.

Mwangi, T., Maina, R., & Waweru, P. (2020). Security technologies and their impact on loss prevention in Kenya's manufacturing sector. *International Journal of Business and Security, 10*(1), 23-35.

Mwangi, T., Maina, R., & Waweru, P. (2020). Security technologies and their impact on loss prevention in Kenya's manufacturing sector. *International Journal of Business and Security, 10*(1), 23-35.

Nairobi County Government. (2021). *Annual Manufacturing Industry Report*. Nairobi County Press.

Odhiambo, R. (2020). Crime Trends in Nairobi: Implications for Business Security in Industrial Areas. *Journal of Urban Crime and Security, 6*(1), 56-76.

Ogolla, M., & Njeri, S. (2020). Industrial security systems and operational efficiency: A case study of Nairobi's Industrial *Area*. *African Journal of Security and Policy, 7*(1), 89-103.

Ogolla, M., & Njeri, S. (2020). Industrial security systems and operational efficiency: A case study of Nairobi's Industrial Area. *African Journal of Security and Policy, 7*(1), 89-103.

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students* (7th ed.). Pearson Education.

Yamane, T. (1967). *Statistics: An Introductory Analysis* (2nd ed.). Harper and Row.