REVIEWED JOURNAL of INTERNATIONAL SOCIAL SCIENCE & HUMANITIES
[ISSN 2663-127X]

Vol. 5, Iss. 1 (2024), pp 223 – 234, April 21, 2024. www.reviewedjournals.com, ©Reviewed Journals

CHALLENGES OF INTEGRATING SURVEILLANCE TECHNOLOGIES AND SECURITY MANAGEMENT BY PRIVATE SECURITY PROVIDERS IN NAKURU COUNTY, KENYA

[1] Anthony Rebo Ngure & [2] Dr. Stephen Handa, PhD

[1] Master of Arts in Security Science and Management, School of Law, Arts and Social Sciences, Kenyatta University, Kenya

[2] Lecturer, Department of Department of Security Diplomacy and Peace Studies, Kenyatta University, Kenya

Accepted: March 28, 2024

ABSTRACT

The study determined challenges of integrating surveillance technologies and security management by private security providers in Nakuru County, Kenya. The study utilized the Integrated System Theory of managing security information. The study adopted a descriptive research design which employed both quantitative and qualitative approaches in collecting and analyzing data which was then analyzed quantitatively and qualitatively. The study targeted private security providers in Nakuru County as unit of analysis. It also employed purposive, stratified, and simple random sampling techniques to select 30 respondents from ten (10) private security providers from the three sub counties distributed among the five sectors of the economy. Interviews and FGDs as well questionnaire were used in the collecting data. Findings indicated that inadequate networks and infrastructure presented additional difficulties for private security companies. Additionally, private security companies faced challenges such improper outcome analysis, corruption, and police intervention during investigations, which made it difficult to find the offenders and resulted in criminals operating freely on the streets. Similarly, security providers encounter technical difficulties such as complex security system installations carried out by unqualified individuals who lack the necessary knowledge and skills; frequent equipment breakdowns, blackouts, malfunctioning equipment, and shortage of qualified technicians. The study concluded that private security companies should use surveillance technologies to suit changing customer demands and keep up with changing crime trends; customers are satisfied with the functionalities of the surveillance technologies and that integrating surveillance technologies is not free of challenges. The study recommended that the police and private security personnel work together to respond to criminal activities and improve the use of surveillance technologies in incident response coordination.

Key Words: *Security Challenges, Surveillance Technologies, security Management*

CITATION: Ngure, A. R., & Handa, S. (2024). Challenges of integrating surveillance technologies and security management by private security providers in Nakuru County, Kenya. *Reviewed Journal of Social Science & Humanities*, 5 (1), 223 – 234.

INTRODUCTION

In the past two decades has seen different socio-economic sector develop and complicated life in various aspects including security and safety of individuals. As a result, the need for their security and monitoring has turned out to be a necessity. Technological surveillance is a term that is now commonly used to describe camera surveillance as far as security is concerned (Elharrouss et al., 2021). It is significantly becoming effective in managing, crime. It is a modern surveillance method for monitoring movements of people and objects in a given area.

Integration of technological surveillance has resulted in different developments in the security industry. It has changed security operations at home security and multi-billion companies. Private security providers are nowadays stringent with their recruitment process with technological knowhow being among the main requirements (Memos et al., 2018). Stergiou et al. (2018) contend that smartphone is increasingly becoming an operation tool and private security companies are partnering with government security officers to prevent and manage crime. Customers have also upped their expectations and expect provision of robust security and a fair price.

Private security firms in East African countries utilize various surveillance technologies such as CCTV cameras, access control systems, biometric systems, and alarm systems. They employ these technologies to enhance security, deter criminal activities, and protect assets. The benefits include improved incident detection, faster response times, increased situational awareness, and a heightened sense of safety. However, challenges include high implementation costs, technological limitations, privacy concerns, and the need for skilled personnel to operate and maintain the systems (Porikli et al., 2013). Despite these challenges, it is not clear how private security providers can harness the use of surveillance technologies to enhance their capabilities and provide effective security solutions.

Overall, conducting a study on the integration of surveillance technologies into security management in Kenya, focusing on private security providers in Nakuru City County, can contribute to the development of more robust and efficient security systems, while also addressing potential challenges and ensuring responsible implementation of these technologies. However, there is a lack of information regarding why private security providers in developing countries integrate surveillance technologies, customer satisfaction with their services, and the challenges they face. This study attempted to fill this gap by examining the integration of surveillance technology by private security providers in Nakuru City County, Kenya.

Statement of the Problem

Technology is revolutionizing the field of security service. For the last four decades, provision of security has witnessed an evolution, from the old-style guard who patrolled premises to the modern security officer who leverages technology, GPS components and real-time digital reporting. In the 20th century, security services evolved to include technology such as CCTV cameras, access control systems, and alarm systems. These technological advancements improved the effectiveness of security officers, enabling them to monitor and respond to security threats more efficiently. The rapid increase of digital technology has led to the development of sophisticated security systems that can detect and deter threats in real time. These systems have transformed the role of security officers from passive observers to proactive responders. Surveillance security cameras, for example, have become a ubiquitous feature of modern security systems. These cameras are capable of capturing high-quality footage in real-time, allowing security officers to monitor and respond to potential security threats. Access control systems have also become more sophisticated, with biometric identification systems and smart cards replacing traditional keys and locks. The foregoing illustrates that adoption of technology has improved efficiency in provision of security in monitoring and response to security

threats as well as the accuracy of security systems. Despite the evident transformative impact of technology in the field of security services globally, private security firms in Nakuru appear to lag behind in the adoption of these advancements. This raises serious concerns about the safety and security of people and property in that area. This study therefore determined the challenges of integrating surveillance technologies by private security providers in Nakuru County. The aim was to proffer the best mechanisms of entrenching the adoption of surveillance technologies in security management in Nakuru and then replicate the same countrywide.

Objective of the Study

The main objective of the study was to explore determine the challenges of integrating surveillance technologies by private security providers in Nakuru County.

LITERATURE REVIEW

Some studies have examined the challenges in integrating technology in organizational operations. For instance, years of experience of a company and staff, level of education, age, and sex have been examined to ascertain whether they influence the adoption and use of technology. A study conducted by Atabek (2019) on integration of technology in education found that experienced staff do not think that hardware or its newness is a barrier to successfully integrating technology in an organization. The study also found that it is not the technologies or gadgets that is a challenge but lack of adequate information and knowledge. This finding is supported by another study conducted by Lowther (2010) who found no association between demographic variables and challenges of integration of technology in an organization. However, lack of any relationship between demographic variables and challenges of integration of technology imply that there are challenges regardless of one's year of experience, job position, and level of education, age, and sex.

Another study by Fischer et al. (2018) found that in-service training insufficiently results in challenges to technology integration in organizations. Keser and Cetinkaya (2013) add that knowledge of how to use a technology is more important than the technology itself. Other studies indicate that staff should be trained routinely to address the knowledge gap in integration of technology (Aatabek, 2019; Inan & Lowther, 2010). Further, another study by Dede (2011) observes that physical infrastructure and sufficiency of technology are essential for successful integration of technology. These studies reveal that poor physical infrastructure, insufficient technologies, and inadequate skills and knowledge are some of the challenges that organizations face in the integration of technology in their operations. However, there is no information on how emerging and established private security providers navigate these challenges and therefore a need to fill this gap.

The majority of police officers in the UK (95%) who took part in Levesley and Martin's (2005) study said that CCTV was the most useful tool for their investigations. This

occurred as a result of CCTV cutting down on the amount of time they had to locate, identify, and apprehend individuals as well as speak with witnesses and suspects. Additionally, almost half (49%) of the police said they have used CCTV to get suspects to admit guilt. However, because CCTV evidence was never good enough to convict criminals, several police voiced their displeasure with its use in court. Hence, the current study intended to assess whether surveillance technology integrated by private security providers helped in proving cases in court in Nakuru City County.

Zheng and Xia (2021) examined private security providers in Kenya and their impact – a case study of Chinese companies. The study found that one of the challenges facing security companies is lack of trained staff and physical infrastructure. The training of staff is often informal and not regular. The study also found that most of the training are not based on technology integration as they mainly involve general risk management education, Chinese language learning, and standard standing posture. However, the study observed a positive aspect that security guards on patrol in some of the Chinese security companies are fitted with body cameras that provide real-time information. Nonetheless, some of the security guards are not adequately equipped to interpret information from the cameras. Nonetheless, there is no evidence on how these

Chinese-owned security providers in Kenya navigated the challenge of training and setting up physical infrastructure and thus the need for this study to fill this gap.

Organizational culture and security awareness is another area with specific challenges. Information security is considered to be one of the aspects of the organizational culture. Studies have demonstrated that not all employees understand the security of the organization as a component of their daily work (Ashenden et al., 2013; Tsohou et al., 2015). The study also observe that private security companies fail to execute security culture in their organizations and those of their clients since there is no uniform understanding of security issues (Ashenden et al., 2013; Tsohou et al., 2015). Other studies note that neglecting security training among organizations and failure of staff to know security rules of organizations is a big challenge as it results in breach of security protocols (Da Veiga 2017; Da Veiga et al. 2010). These studies only highlight the challenges facing private security companies but fall short on how these challenges can be addressed necessitating the need for this study.

The College of Policing (2019) states that there are various methods in which police officers' incapacity to use CCTV in their work might be demonstrated. These can include failing to recognize or address noteworthy situations, apprehending suspects, being unable to analyze video, or losing legal battles as a result of improper management of video. For instance, a study conducted in the USA by Goodison et al. (2015) discovered that a shortage of appropriately educated analysts caused police to face a backlog in the analysis of digital evidence, including CCTV footage. Similarly, Yau (2019) found that a major obstacle to maintaining CCTV systems was a shortage of skilled professionals in a study on the use of CCTV in crime detection in Nigeria. These studies, however, only highlight the challenges of integrating modern surveillance technologies, only focuses on police officers, and were conducted in countries with different demographics compared to Kenya. Therefore, this study was needed to identify the challenges faced by private security companies, offer localised solutions, and contextualize the findings for private security providers in integration of surveillance technologies.

Apart from users' competences, some studies consider vandalism of CCTV equipment and accessories a serious challenge to adopting CCTV in managing crime (La Vigne et al., 2011a; Keval, 2009). Vandalism is the deliberate destroying or damaging of property. Vandals may target CCTV systems for tactical purposes, such as vengeance, attitude expression, or profit-making part sales. CCTV components can be vandalized in a variety of ways, such as purposefully removing the cameras and fixtures, severing cables, breaking cameras, changing their viewing angles, or painting them black with paint or other materials. According to La Vigne et al. (2011a), vandalism of CCTV equipment and accessories results in increased maintenance and repair expenses, which ultimately lowers the efficacy of CCTV systems. These findings informed the current study to establish whether private security providers in Nakuru County experienced similar challenges and offer suitable recommendations.

Keval (2009) discovered that because criminals had vandalized certain CCTV, it was unable to assist UK police in keeping an eye on public areas. It was vital to ascertain whether CCTV vandalism occurred and hampered security management in Nakuru County. According to Cuevas et al. (2016), one major obstacle to the use of CCTV in crime solving is police personnel' disinterest in the technology. According to Piza et al. (2016), many police organizations find the expense of setting up and maintaining CCTV systems to be relatively high. This is due to the fact that substantial resources are needed for the installation and upkeep of CCTV infrastructure, the salary of CCTV operators, and the management of an increase in the number of crimes that are reported to the police. Furthermore, the integration of technologies like ALPR or the need for huge storage capacity for video result in increased expenses associated with maintaining CCTV (La Vigne et al., 2011b). These factors help to explain why some security providers have not yet purchased CCTV equipment while others have stopped using it (Schuck, 2015). Harris and Harris (2009) contend that despite these difficulties, the high cost of installation and upkeep of CCTV systems can be justified if they give the

desired results. Therefore, it was necessary to establish whether the availability of funds has negatively impacted integration of surveillance technology in Nakuru City County.

Shortage of electrical supply and crooks avoiding detection on CCTV cameras are two more challenges that have reported by studies. For example, Lindegaard and Bernasco (2018) and Gill and Loveday (2003) demonstrated that criminals might conceal their identities from CCTV cameras in order to avoid being caught. On the other hand, Yau (2019) discovered that CCTV footage loss in Nigeria was frequently caused by an inadequate power supply. Investigating whether these challenges have impacted the integration of surveillance technology in Nakuru County was therefore imperative.

It is also expensive to acquire and maintain security technologies. Access control, Video Surveillance Systems (VSS), and Intrusion Detection System (IDS) are key security systems. According to British Security Industry Association (2017), acquiring, operating, and maintaining these systems separately is expensive. Further, Musyoka (2016) notes that it notes that training, administration, and service maintenance of these systems is expensive. These studies only highlight how expensive it is to install and maintain modern surveillance technologies by the police but fall short on private security providers and do not provide possible solutions to these challenges thus the need for this study.

Theoretical Framework

The Integrated System Theory

The Integrated System Theory of managing security information will be used in this study. The theory is derived from five fundamental theories namely contingency theory, management system theory, control and audit theory, risk management theory, and the information policy theory (Soomro, Shah, & Ahmed, 2016). According to Knowles et al. (2015), this theory makes sure that confidentiality and integrity of operational procedures and data in an organization is maintained. It also ensures that there is protection of information when using combined systems, internal controls, and operations (Hong, 2003). The theory assumes that organizations have the ability of determining vulnerability and threats after evaluating security risks (Raid & Floyd 2006).

The theory was selected because it focuses on planning security needs in an organization, formulating security policies, and developing strategies for executing security strategies (Somro et al., 2016). Further, it was selected because it underscores security control assurance where organizations continuously analyze security risks, assess security risks, vulnerabilities, manages risks, and audits security to eliminate security gaps using different strategies including private security providers (Kassan, 2021). This aspect is well captured in the contingency theory which is part of the integrated system theory. The theory can also help in understanding how organizations deter, prevent, and respond to security threats and the challenges they encounter (Hossein et al., 2021).

This theory, therefore, entails three fundamental components of data protection namely internal controls and procedures, operations, and combined systems (Kassan, 2021). These components are essential in assessing information security management systems in any organization that has contracted private security providers. For instance, the combined system components influence how the organizations plans their windows, doors, security officers, gates, and walls. Sandberg, Amin, and Johansson, (2015) note that it is also concerned with how these security barriers linked to electronic security measures such as CCTV cameras and alarms are using established network. Operation component suggests that security activities in place inform data protection. This concept will help the study assess plans put in place by private security providers to protect their customers and their properties.

Further, procedures are essential in security management as highlighted in the theory. It is important that private security providers are guided in their operations (Kassan, 2021). Thus, this theory emphasizes contingency plans, strategies, planning, use of policies, and continuous review of policies which are

associated with customer satisfaction. This element will help the researcher assess security management information procedures in private security companies in line with their guidance manuals and existing policy frameworks. It will also help the researcher understand the reasons for private security providers integrating surveillance technologies, customer satisfaction, and the challenges of integrating surveillance technologies in security management.

Conceptual Framework

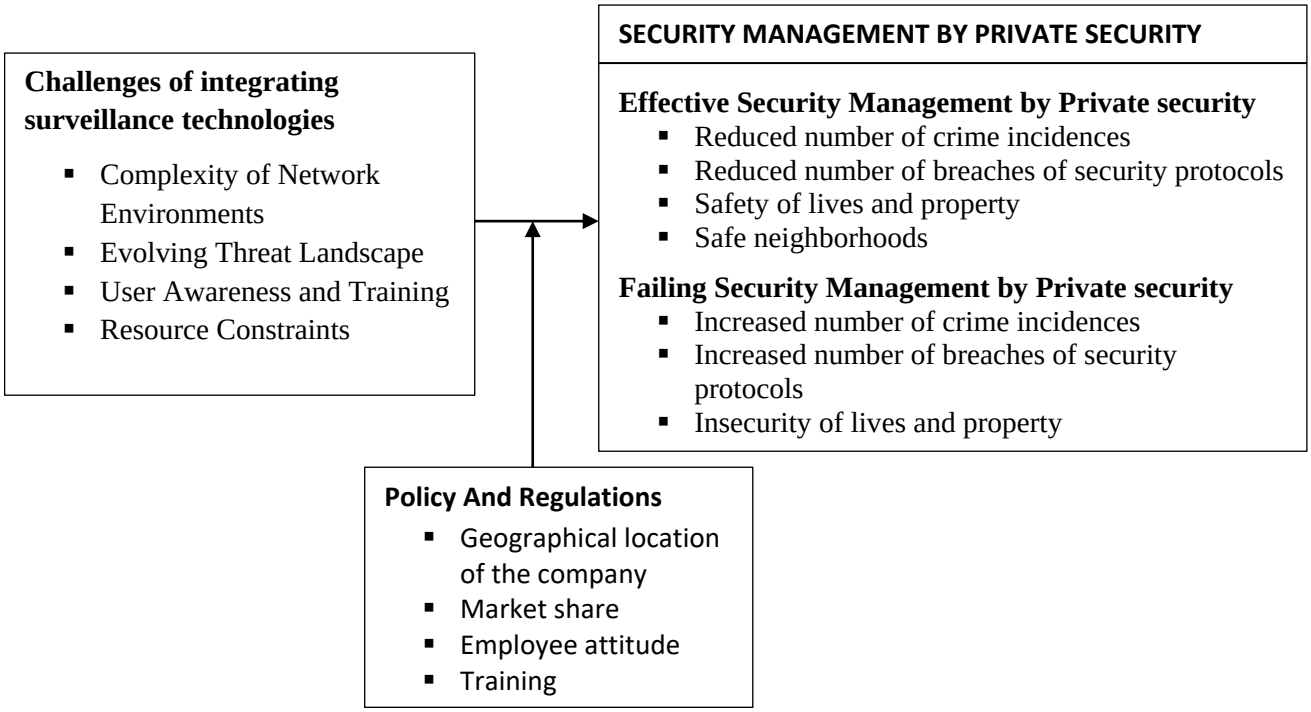

Figure 1: Conceptual Framework

METHODOLOGY

This study employed a descriptive research design. The study was conducted in Nakuru City County. Nakuru City County is within the former Rift-valley province. Nakuru County has 11 Sub-counties, with Nakuru Town which was elevated recently to a city status being a host to Nakuru West and Nakuru East Sub-counties. The study area was selected because it is densely populated, the socio-economic challenges made crime the order of the day hence the need for surveillance. The target population of this study was private security providers in Nakuru City County, the consumers of the services in different category eg. Residentials, shopping malls, Retail outlets like Supermarkets, Hospitality Industry like Hotels, Schools, and Hospitals. The study targeted private security companies registered by the Kenyan government and vetted by the Private Security Regulatory Authority (PSRA) and contracted by individuals or businesses to provided security. The study used purposive, stratified, and simple random sampling techniques to arrive at a sample size. This study used a sample size of 30 respondents evenly spread in the 10 private security companies, in five sectors of the economy, and in the three sub counties.

The study utilized three research instruments for the collection of the primary data. The research instruments were: a) the survey questionnaire: to gather information from the targeted respondent b) In-depth Interview guide for the Focus Group Discussions to explore and gather detailed insights on specific topic and c) Interview guide for the Key Informants. The interviews were guided by the interview guide as a data collection tool. Interview guide was selected as a data collection tool in this study because it created a structured process; it was easier to assess every respondent in the same way thus reducing bias; and all

respondents are exposed to the same experience (Kallio et al., 2016; Turner III & Hagstrom-Schmidt, 2022). Secondary data was collected through content analysis. The questionnaires were administered to the identified sample size of 30 respondents across the 10 private security companies, in five sectors of the economy, and in the three sub-counties. The questionnaires were issued to the respondents and collected on the following day from each of the respondents.

Quantitative data about the socio-demographic characteristics of the respondents was analyzed quantitatively using excel. Microsoft Excel is effective in analyzing and presenting basic quantitative data such as age, marital status, and education level among others (Bree & Gallagher, 2016). Qualitative data was analyzed qualitatively using thematization. The data were analyzed to identify themes in the responses. The researcher examined the participants' responses multiple times to identify themes. He also examined responses per research objectives to identify themes for analysis. Therefore, themes were identified manually and organized for analysis and presentation.

FINDINGS AND DISCUSSION

Challenges of Integrating Surveillance Technologies

This section presented the results of the third specific objective of the study, which sought to determine the challenges of integrating surveillance technologies by private security providers in Nakuru City County. The information on this objective was collected using questionnaires which had statements which were rated on a five-point Likert scale, 1- strongly disagree, 2-Disagree, 3-Undecided 4-Agree, 5-Strongly agree, against which the respondents were asked to tick the correct choice. More information on the same issue was collected through Focus Group Discussions and interviews. The results are presented in table 1.

Table 1: Respondents' Views on Challenges of Integrating Surveillance Technology

Measure	1	2	3	4	5	Mean
The private security providers experience challenges which affect the quality of security services provided to clients	-	1 (3.7%)	3 (11.1%)	4 (14.8%)	**19 (70.4%)**	3.46
Private security providers encounter technical challenges when integrating surveillance technology	-	2 (7.4)	1 (3.7%)	1 (3.7%)	**23 (85.1%)**	3.64
There are financial challenges associated with integration of various surveillance technologies by private security providers	-	-	3 (11.1%)	**19 (70.4%)**	5 (18.5%)	2.84
There are regulatory/legal challenges that private security providers face when integrating surveillance technologies		1(3.7%)	-	5 (18.5%)	**21 (77.7%)**	3.72

Note: 1-strongly disagree, 2-Disagree, 3-Undecided, 4-Agree, 5-Strongly agree

The results on table 1 indicated that majority 21 (77.7%) of the respondents strongly agreed that there are legal challenges that private security providers face when integrating surveillance technologies as indicated by a response mean of 3.72. Similarly, majority 23(85.1%) of the respondents strongly agreed that private security providers encounter technical challenges when integrating surveillance technology as indicated by a mean response of 3.64. In addition, majority of the respondents 19 (70.4%) strongly agreed that the private security providers experience challenges which affect the quality of security services provided to clients with a response mean of 3.46. Further, the majority 19(70.4%) agreed that there are financial challenges associated with integration of various surveillance technologies by private security providers.

These findings imply that the private security providers experience legal, financial and technical challenges when integrating surveillance technologies in security management in Nakuru City County. Similar reports

were submitted by respondents during interviews and focus group discussion:

Private security providers are challenged by high costs of maintenance and installation. In addition to that, training can be cumbersome and time consuming to the employees. Also, power disruptions sometimes create loopholes that may render the technology ineffective *(Key Informant I, 2023)*

Some equipments are stolen or disabled by experienced criminals, thus no evidence will be available in such cases. In addition, the technological equipment is costly for low budget businesses. Also, there may be inconveniences caused due malfunctions or complexities of installation

(Key Informant II, 2023)

Sometimes the security providers may experience technical challenges during the integration of surveillance technology such as installation of complex security systems by unqualified personnel who lack the required knowledge and skills on how to install them *(Key Informant III, 2023)*

They experience financial challenges because effective security systems are quite costly in their purchases, installation and maintenance. Further, there is lack of trained manpower that are also expensive to pay and technology failures *(Key Informant IV, 2023)*

FGD participants also reported:
Most of the security companies are still growing so they experience financial challenges in installing and maintaining effective security systems *(Participant A4, FGD 1, 2023).*

Yes, there are technical challenges like incompatibility of some technologies or some of the equipment is outdated which requires the security provider a whole overhaul of the surveillance system which turn out very costly *(Participant B4, FGD 2, 2023).*

Sometimes there are technical challenges such as faulty alarms especially when there is a blackout. Yes, sometimes we get incompetent technicians who are not sure about the scope of work and the equipment should installed and operated effectively *(Participant C4, FGD 3, 2023).*

Yes. Some of the challenges include failure of the equipment, power blackouts and poor network connectivity *(Participant D4, FGD 4, 2023).*

Lack of proper analysis of outcomes, follow up of culprits takes a long time and inadequate resources for repair and maintenance *(Participant E4, FGD 5, 2023).*

Corruption and police interference during investigations leads to criminals walking freely on the streets *(Participant A5, FGD 1, 2023).*

Poor network and infrastructure, frequent breakdown of equipment due to weather challenges like a lot of rain/dust *(Participant B5, FGD 2, 2023).*

There are legal challenges i.e the privacy and data protection act, where some people do not want their information shared and if you do that, they can sue you. They are subjected to legal actions if their devices are not well maintained and if they are not accountable for security concerns *(Participant C6, FGD 3, 2023).*

It is evident that private security providers experience challenges when integrating surveillance technologies. Some of the challenges include high costs of installation and maintenance of the equipment, Vandalism, poor infrastructure and technical challenges like frequent breakdown of equipment due to bad weather, power black outs, faulty equipment and lack of qualified technicians. These findings are in line with the findings reported by Atabek (2019) that it is not the technologies or gadgets that is a challenge but lack of adequate personnel with adequate information and knowledge. This finding is supported by another study conducted by Lowther (2010) who found an association between challenges of integration of technology in an organization and quality of services provided.

The results also support the conclusions of Keser and Cetinkaya (2013), who stated that technical proficiency is more significant than actual technology. According to other research, employees should receive regular training to close the knowledge gap in technology integration (Aatabek, 2019; Inan & Lowther, 2010). Dede (2011) notes in another study that enough technology and a physical infrastructure are necessary for effective technological integration. These studies show that some of the difficulties that companies encounter when integrating technology into their operations are inadequate technologies, limited skills and expertise, and bad physical infrastructure.

On the same breath, Zheng and Xia (2021) looked at Kenyan private security companies and their effects on a Chinese company case study. According to the report, one issue security organizations face is a shortage of physically equipped and trained personnel. Employee training is frequently irregular and unstructured. The survey also discovered that some security guards lack the necessary tools to properly interpret footage from the cameras, and that the majority of training programs do not integrate technology because they focus primarily on general risk management education.

The findings also confirm the conclusions published by the College of Policing (2019), which said that police officers' incapacity to effectively use CCTV in their work can take many different forms. These can include failing to recognize or address noteworthy situations, apprehending suspects, being unable to analyze video, or losing legal battles as a result of improper management of video. For instance, a research conducted in the USA by Goodison et al. (2015) discovered that a shortage of appropriately educated analysts caused police to face a backlog in the analysis of digital evidence, including CCTV footage. Similarly, Yau (2019) found that a major obstacle to maintaining CCTV systems was a shortage of skilled professionals in a study on the use of CCTV in crime detection in Nigeria.

According to various research, vandalism of CCTV equipment and accessories poses a serious risk to the use of surveillance technologies in managing crime, independent of user competence (La Vigne et al., 2011a; Keval, 2009). Vandalism is the deliberate destroying or damaging of property. Criminals may intentionally damage security equipment to convey a message, get revenge, or profit financially from the sale of parts. Component vandalism can take many different forms, including as purposefully removing the cameras and fixtures, severing wires, breaking cameras, changing their viewing angles, or spray-painting or otherwise darkening them. According to La Vigne et al. (2011a), vandalism of CCTV equipment and accessories results in increased maintenance and repair expenses, which ultimately lowers the efficacy of CCTV systems.

Similar results were published by Lindegaard and Bernasco (2018), who noted that two issues raised by CCTV study are criminals turning off CCTV cameras and a shortage of power. In a similar vein, Gill and Loveday (2003) demonstrated that criminals could disguise their identities in order to avoid being seen by CCTV cameras. On the other hand, Yau (2019) discovered that CCTV footage loss in Nigeria was frequently caused by an inadequate power supply. In the same sentence, the British Security Industry Association (2017) stated that it is costly to purchase, run, and maintain security systems alone. This confirms that security providers have difficulties due to vandalism, inadequate power supply or blackouts, and high maintenance expenses associated with surveillance gear.

CONCLUSIONS AND RECOMMENDATIONS

The objective of the study was to determine the challenges of integrating surveillance technologies by private security providers in Nakuru City County. It was evident that private security providers experience challenges when integrating surveillance technologies. Some of the challenges included high costs of installation, inadequate resources for repair and maintenance, vandalism and disabling of the equipment by experienced criminals, which prevents the availability of evidence necessary for an inquiry. In addition, the findings indicated that inadequate networks and infrastructure presented additional difficulties for private security companies. Additionally, the study found that private security companies faced challenges such improper

outcome analysis, corruption, and police intervention during investigations, which made it difficult to find the offenders and resulted in criminals operating freely on the streets. Finally, the study found that security providers encounter technical difficulties when integrating surveillance technology. These difficulties include complex security system installations carried out by unqualified individuals who lack the necessary knowledge and skills, as well as frequent equipment breakdowns brought on by inclement weather, blackouts, malfunctioning equipment, and shortage of qualified technicians to perform maintenance.

Based on the findings, the study concluded that integrating surveillance technologies presented several challenges for private security providers. These challenges included: high costs of installation, inadequate resources for repair and maintenance, frequent breakdown of equipment, vandalism and or disabling of the equipment by experienced criminals, black outs, lack of trained personnel, poor network, corruption, and police intervention during investigations that resulted in fruitless investigations. The researcher noted that the issues of privacy came up during the interview, it is well to note that the government has tried to address the issue of privacy through the introduction of the Data Protection Act, 2019. This as noted, not many clients and companies appreciate the challenges and the exposure thereof. There is need for the companies to train their employees and clients, on what exactly the Act is all about to avoid legal challenges.

Based on the conclusions, the study recommended that in order to prevent disputes in functional areas of responsibility, police and private security personnel should work together to respond to occurrences recorded on surveillance technologies and improve the use of surveillance technologies in incident response coordination. Additionally, corrupt police officials who interfere with evidence should be brought to book and face the law. Also, police officers and private security companies that use CCTV cameras should organize regular meetings. This would make it easier to communicate and provide feedback, especially on experiences and suggestions for improving the County's use of surveillance technologies to reduce crime. In addition, this would improve the working connections between the two groups and aid in finding answers to current issues when coordinating responses to occurrences captured on camera. Corrupt police officers who tamper with evidence should also be held accountable and prosecuted. Lastly, private security companies in collaboration with the police should regularly educate the public about the advantages of integrating surveillance technology into security management as well as the efficient ways to use it. Programs for sensitization may involve simulated training to give guards, employees, and clients information and expertise on camera monitoring, as well as hands-on experience in incident response coordination for those working in the field.

Recommendations for Further Research

In light of this study's limitations and scope, further research may focus on the following topics:

- Similar studies should be conducted in other counties and the results compared.
- Thorough and comprehensive grasp of the ways that surveillance technology affects security management.
- Evaluate the usefulness of government-run surveillance systems in Nakuru City County. This is due to the fact that the current study only examined the integration of surveillance technologies by private security companies.
- Global Perspectives: Compare how different countries handle the integration of surveillance technologies by private security firms, considering cultural and legal variations.
- Cost-Benefit Analysis: Conduct a cost-benefit analysis to understand the economic implications of implementing integrated surveillance systems for private security.

REFERENCES

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy?. *Computers & Security*, *39*, 396-405. Retrieved from: https://www.sciencedirect.com/science/article/abs/pii/S0167404813001338

Atabek, O. (2019). Challenges in integrating technology into education. *arXiv preprint arXiv:1904.06518*. Retrieved from: https://arxiv.org/abs/1904.06518

Bree, R. T., & Gallagher, G. (2016). Using Microsoft Excel to code and thematically analyse qualitative data: a simple, cost-effective approach. *All Ireland Journal of Higher Education*, *8*(2). Retrieved from: https://ojs.aishe.org/index.php/aishe- j/article/view/281

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & security*, *29*(2), 196-207. Retrieved from: https://www.sciencedirect.com/science/article/abs/pii/S0167404809000923

Dede, C. (2011). Reconceptualizing technology integration to meet the necessity of transformation. *Journal of Curriculum and Instruction*, *5*(1), 4-16. Retrieved from: http://www.joci.ecu.edu/index.php/JoCI/article/view/121

Elharrouss, O., Almaadeed, N., & Al-Maadeed, S. (2021). A review of video surveillance systems. *Journal of Visual Communication and Image Representation*, *77*, 103116. Retrieved from: https://www.sciencedirect.com/science/article/abs/pii/S1047320321000729

Fischer, C., Fishman, B., Dede, C., Eisenkraft, A., Frumin, K., Foster, B., ... & McCoy, A. (2018). Investigating relationships between school context, teacher professional development, teaching practices, and student achievement in response to a nationwide science reform. *Teaching and Teacher Education*, *72*, 107-121. Retrieved from: https://www.sciencedirect.com/science/article/abs/pii/S0742051X17314130

Githae, A. A. W. (2019). *Utilisation And Effectiveness Of Outsourced Private Security Services By Commercial Banks In Kenya* (Doctoral dissertation). Retrieved from: http://41.89.227.156:8080/xmlui/handle/123456789/4614

Hagen, J., & Albrechtsen, E. (2009). Effects on employees' information security abilities by e- learning. *Information Management & Computer Security*, *17*(5), 388-407. Retrieved from: https://www.emerald.com/insight/content/doi/10.1108/09685220911006687/full/h tml

Hancock, D. R., Algozzine, B., & Lim, J. H. (2021). Doing case study research: A practical guide for beginning researchers. Retrieved from: https://books.google.co.ke/books?hl=en&lr=&id=G3FEEAAAQBAJ&oi=fnd&pg=PP1&dq=Hancock,+D.+R.,+Algozzine,+B.,+%26+Lim,+J.+H.+(2021).+Doing+case+study+research:+A+practical+guide+for+beginning+researchers.&ots=iqU6rwUY6f&sig=fzwIYq7MdnPLpnuNqUTDOYCsS-E&redir_esc=y#v=onepage&q&f=false

Hossein Nezhad Nedaei, B., Abdul Rasid, S. Z., Sofian, S., Basiruddin, R., & Amanollah Nejad Kalkhouran, A. (2015). A Contingency-Based Framework for Managing Enterprise Risk. *Global Business and Organizational Excellence*, *34*(3), 54-66. Retrieved from: https://onlinelibrary.wiley.com/doi/full/10.1002/joe.21604

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of advanced nursing*, *72*(12), 2954-2965. Retrieved from: https://onlinelibrary.wiley.com/doi/full/10.1111/jan.13031

KASSAN, P. L. (2021). Use of integrated security management system in crime prevention: a case of public referral hospitals in nairobi city county, kenya.

Keser, H., & Çetinkaya, L. (2013). ÖĞRETMEN VE ÖĞRENCİLERİN ETKİLEŞİMLİ TAHTA KULLANIMINA YÖNELİK YAŞAMIŞ OLDUKLARI SORUNLAR

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security

management in industrial control systems. *International journal of critical infrastructure protection*, *9*, 52-80. Retrieved from: https://www.sciencedirect.com/science/article/abs/pii/S1874548215000207

Marshall, D., Thomas, T., Marshall, D., & Thomas, T. (2017). Photographs, CCTVs and Other Cameras. *Privacy and Criminal Justice*, 127-151. Retrieved from: https://link.springer.com/chapter/10.1007/978-3-319-64912-2_6

Memos, V. A., Psannis, K. E., Ishibashi, Y., Kim, B. G., & Gupta, B. B. (2018). An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework. *Future Generation Computer Systems*, *83*, 619-628.

Neuendorf, K. A. (2017). *The content analysis guidebook*. sage. Retrieved from: https://books.google.co.ke/books?hl=en&lr=&id=nMA5DQAAQBAJ&oi=fnd&pg=PP1&dq=Neuendorf,+K.+A.+(2017).+The+content+analysis+guidebook.+sage.&ots=pIMkw3jz6r&sig=2aH_LKepCqrrUqqhMKr8C6J3TDA&redir_esc=y#v=onepage&q&f=false

Patel, R. (2021). A study on customer perception towards cctv security system. *Patel Institute of BMC & IT*, Uka Tarsadia University.

Porikli, F., Bremond, F., Dockstader, S. L., Ferryman, J., Hoogs, A., Lovell, B. C., ... & Venetianer, P. L. (2013). Video surveillance: past, present, and now the future [DSP Forum]. *IEEE Signal Processing Magazine*, *30*(3), 190-198.

Sandberg, H., Amin, S., & Johansson, K. H. (2015). Cyberphysical security in networked control systems: An introduction to the issue. *IEEE Control Systems Magazine*, *35*(1), 20-23. Retrieved from: https://ieeexplore.ieee.org/abstract/document/7011179

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management*, *51*(2), 217-224.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International journal of information management*, *36*(2), 215-225. Retrieved from: https://www.sciencedirect.com/science/article/abs/pii/S0268401215001103

Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, *78*, 964-975. Retrieved from: https://www.sciencedirect.com/science/article/abs/pii/S0167739X1630694X

Turner III, D. W., & Hagstrom-Schmidt, N. (2022). Qualitative interview design. *Howdy or Hello? Technical and Professional Communication*. Retrieved from: https://pressbooks.library.tamu.edu/howdyorhello/back-matter/appendix-qualitative-interview-design/

Wilson, C., Hargreaves, T., & Hauxwell-Baldwin, R. (2017). Benefits and risks of smart home technologies. *Energy Policy*, *103*, 72-83. Retrieved from: https://www.sciencedirect.com/science/article/pii/S030142151630711X/?science2

Zheng, S., & Xia, Y. (2021). Private Security Companies in Kenya and the Impact of Chinese Actors. *Available at SSRN 3859591*. Retrieved from: https://www.sciencedirect.com/science/article/abs/pii/S0747563217300791