EAST AFRICAN JOURNAL OF CRIME AND SECURITY

JOURNAL ARTICLE

VOLUME 1, ISSUE 2 | PAGES 1-10

The Role of Security Guards' Technological Competency in Client Perceptions of Security Service Effectiveness

Silas Muriira Killingo

https://doi.org/10.66699/fy7qr107

ABSTRACT

Private security provision in East African cities increasingly depends on emergent surveillance and access-control technologies, yet the value these systems generate is mediated by the people who operate them. This paper examines the relationship between the level of technological competency among front-line private security guards and the perceived level of security among the clients they serve, drawing on mixed-methods survey and key-informant data collected from private security providers operating in Nairobi's Industrial Area. The paper argues that technology adoption figures overstate operational readiness, because certification, training frequency, and self-rated competency vary sharply across technology types and remain the binding constraint on perceived security outcomes. Correlational evidence indicates that competency and certification are more strongly associated with client-perceived security than the mere presence of a technology. The paper concludes that private security governance in Kenya should shift emphasis from procurement toward structured, continuous competency-building, and it identifies the conditions under which this relationship is likely to hold or break down.

Keywords: situational crime prevention; private security; surveillance technology; Nairobi; opportunity reduction

How to Cite:

Killingo, S. M. (2026). The role of security guards' technological competency in client perceptions of security service effectiveness. *East African Journal of Crime and Security*, 1(2), 1–10. https://doi.org/10.66699/fy7qr107

1. INTRODUCTION

1.1 Background of the Study

The private security industry has become an indispensable extension of urban public safety infrastructure across much of the world, filling operational gaps left by resource-constrained public police forces (Paddy, 2006). Emergent technologies such as closed-circuit television, biometric access control, global positioning system tracking, and artificial-intelligence-assisted surveillance are now marketed as the principal lever through which private providers can compensate for these gaps, promising real-time situational awareness and a more proactive security posture than traditional guarding alone can deliver. Across Sub-Saharan Africa, however, the diffusion of these tools has proceeded unevenly, shaped less by the sophistication of the technology itself than by the institutional and human capacity available to operationalise it (Abrahamsen & Williams, 2011).

Kenya illustrates this tension vividly. The country's private security sector expanded rapidly from an informal, loosely regulated activity in the 1970s and 1980s into a formally licensed industry following the Private Security Regulation Act, reflecting both rising urban crime and the state's incapacity to police it unaided (Diphoorn, 2016; Mutuma & Pommerolle, 2003). Nairobi, as the country's commercial and logistical hub, sits at the centre of this transformation. Its Industrial Area concentrates manufacturing plants, customs bond yards, and warehousing operations whose asset density makes them attractive targets for organised theft and vandalism. Private providers operating in this zone have consequently invested heavily in surveillance and access-control infrastructure, positioning themselves as the de facto guarantors of commercial security where public policing capacity is stretched thin (Mohamed, 2022).

Yet acquiring a technology is analytically distinct from using it competently. A growing regional literature suggests that continuous professional development, technical certification, and routine familiarity are the binding constraints on whether digital security tools translate into measurable safety gains, particularly where infrastructural conditions, such as unreliable power and constrained connectivity, already complicate deployment (Arakpogun, Elsahn, Nyuur, & Olan, 2020; Naatu, Selormey, & Naatu, 2025). Kenyan private security personnel, drawn predominantly from a workforce with limited formal technical training, are frequently asked to operate systems whose effective use presumes a level of digital literacy the sector has not systematically cultivated (Akoch, 2021). This creates a plausible yet underexamined human-capital bottleneck between technological investment and the security outcomes clients ultimately experience and evaluate.

1.2 Problem Statement

Nairobi's Industrial Area has recorded a disproportionate rise in criminal activity compared with other parts of the city, with reported incidents increasing by approximately 18% over a single year, compared with considerably lower increases in the Central Business District and Westlands (Kenya National Bureau of Statistics, 2022). Conventional public policing instruments, including manual patrol and basic closed-circuit monitoring, have proven increasingly inadequate against more sophisticated and mobile criminal tactics, a shortfall that has pushed commercial and industrial occupiers toward private providers equipped with newer surveillance and access-control systems. Existing accounts of this shift, however, tend to treat “technology adoption” as a binary and self-explanatory variable: a firm either has biometric access control or it does not, has closed-circuit television or does not, with little systematic attention paid to whether the personnel deploying these systems possess the competency required to use them effectively, or whether that competency is what clients are actually responding to when they report feeling safer.

This gap matters because policy and investment decisions in the sector are presently oriented around procurement rather than personnel. If perceived security is driven substantially by guard competency rather than by the presence of a technology per se, then capital directed solely at acquiring new surveillance infrastructure, without a commensurate and sustained investment in training and certification, is likely to under-deliver on its promised security dividend. Conversely, if competency proves to be only weakly associated with perceived security once a technology is in place, this suggests

that visibility and deterrence effects, rather than operator skill, are doing the analytical work, with quite different implications for how firms and regulators should allocate scarce resources. This paper empirically addresses this question.

The claim advanced in this paper is that the security guards' level of technological competency, encompassing certification, training exposure, and operational proficiency, is a stronger and more consistent predictor of client-perceived security than the simple presence or breadth of technology adoption, and that the private security sector in Nairobi's Industrial Area is currently under-investing in this human-capital dimension relative to its stated reliance on it.

2. LITERATURE REVIEW

The literature on private security modernisation in East Africa converges on a broadly consistent narrative: technological uptake among providers has outpaced the institutional mechanisms required to translate that uptake into professional competency. Kenya's regulatory architecture, formalised through licensing and oversight following decades of informal, loosely supervised provision, has succeeded in legitimising the sector as a security actor but has been considerably less effective at standardising the technical skills base of its frontline workforce (Diphoorn, 2016). This regulatory asymmetry, between formalising who may provide security and specifying how competently they must do so, recurs as an explanatory thread across studies of the sector and is consistent with the sector's origins as a response to state incapacity rather than a deliberately engineered professional service (Mutuma & Pommerolle, 2003).

A second, closely related strand of scholarship treats technological competency as embedded within, rather than separate from, broader questions of digital infrastructure and governance in African contexts. Studies of digital-technology adoption across Sub-Saharan Africa consistently identify infrastructural constraints, unreliable power supply, uneven connectivity, and scarce technical support, as conditions that depress the realised value of any given technology investment irrespective of the underlying tool's sophistication (Arakpogun et al., 2020; Naatu et al., 2025). Read against the private security context, this suggests that competency deficits observed among Kenyan guards are unlikely to be a purely sectoral phenomenon; they plausibly reflect a wider national pattern in which digital tools are procured faster than the surrounding technical ecosystem, including training pipelines, maintenance capacity, and institutional support, can mature to support them. This reframes technological competency less as an individual failing of guards and more as a structural outcome of how digital transformation has proceeded across the region.

A third body of work interrogates the accountability and governance dimension of security digitisation, arguing that as Kenyan firms integrate surveillance and biometric tools into client-facing services, questions of data handling, oversight, and professional standards become inseparable from questions of technical competency (Jili, 2022). Where certification and training are weak, this literature suggests, the risks extend beyond operational underperformance to encompass governance failures, including inconsistent data handling and inadequate incident documentation, that further erode the trust relationship between provider and client. This connects competency not merely to functional effectiveness but to the legitimacy of private security as an institution, a link largely absents from studies that measure technology adoption without reference to how it is governed in use.

A fourth and more direct strand addresses the guard-level relationship between skill and security outcomes. Kenyan-focused studies of information-system security practice emphasise that the effectiveness of any monitoring or access-control system depends on the practices, training, and vigilance of the personnel who operate it, rather than on the system's specifications (Njoroge, Ogalo, & Ratemo, 2021). Sector-specific research on Kenyan private security personnel reinforces this, finding that competence gaps are most acute for newer, more technically demanding tools, such as artificial-intelligence-assisted surveillance and biometric access control, and comparatively modest for long-established, simpler technologies such as closed-circuit television, implying that competency deficits scale with technological novelty rather than remaining uniform across a firm's technology portfolio (Akoch, 2021). Not all findings point in the same direction, however: some accounts caution that certification and technical training are necessary but not sufficient conditions for improved outcomes,

arguing that credentials achieve little without accompanying operational integration, supervisory reinforcement, and systemic organisational support (Gawande et al., 2017). This qualification is analytically important because it resists a simplistic “train more, achieve more” reading of the competency literature and instead positions competency as one input among several organisational conditions that jointly determine whether technology delivers a security dividend.

Taken together, this literature converges on three propositions that structure the present study. First, technology adoption and personnel competency are conceptually and empirically distinct variables that existing sectoral accounts too often conflate. Second, competency deficits in the Kenyan private security workforce are patterned, concentrated in newer and more technically demanding tools rather than distributed evenly, and are plausibly rooted in wider national infrastructural and governance conditions rather than firm-level negligence alone. Third, while a consensus exists that competency matters, its relationship to client-perceived outcomes, rather than internally reported effectiveness, remains comparatively under-tested, particularly in high-crime commercial districts such as Nairobi's Industrial Area, where the present study is situated.

3. METHODOLOGY

3.1 Research Design and Study Site

The study employed a mixed-methods design, combining a structured quantitative survey with qualitative key-informant interviews, because the research question required both statistical generalisability regarding competency-outcome associations and contextual depth on how competency is experienced and valued by clients and providers. The study site was Nairobi's Industrial Area, a commercial and manufacturing district that recorded a markedly higher year-on-year rise in reported crime than comparable parts of the city, making it an analytically appropriate setting in which to examine whether technological competency, rather than technology presence alone, is associated with client-perceived security.

3.2 Population, Sampling and Sample Size

The study population comprised security personnel, including security guards, safety surveillance officers, and event security officers, employed by private security providers operating in the study area, as well as corporate security managers and clients engaged as key informants. To preserve the confidentiality of the participating organisations, individual firms are not named in this paper; providers are instead referenced by an anonymised tier designation reflecting firm size and market reach, namely Tier 1 (large, more than 1,100 employees and national or international coverage), Tier 2 (medium, 100 to 1,000 employees), and Tier 3 (small, fewer than 100 employees and localised operations).

The survey sample size was calculated using Cochran's formula for large populations, applied to an estimated population of 157 registered private security firms in the study area, at a 95 per cent confidence level and a five per cent margin of error, yielding an initial sample of 384 respondents. This figure was adjusted downward using the finite population correction formula, given the comparatively small and known population size, producing a final target sample of 217 respondents. Stratified random sampling was then applied across the three provider tiers, proportionate to their estimated population share of fifty, thirty, and twenty per cent for small, medium, and large firms respectively, with firms and respondents randomly selected within each stratum to minimise selection bias. A complementary purposive sample of eight key informants, comprising four corporate security managers, two clients, and two senior security guards, was recruited to provide qualitative depth on the mechanisms linking competency to perceived security.

3.3 Data Collection Instruments

Quantitative data were collected using a structured survey questionnaire administered electronically to security personnel across the sampled tiers, capturing training frequency, certification status by technology type, self-rated competency, frequency of technology use in daily operations, and client-

facing agreement statements regarding the perceived effect of competency on security outcomes. Qualitative data were collected through semi-structured key-informant interviews with corporate security managers and clients, using open-ended prompts designed to elicit contextual perspectives on how technological proficiency among guards shapes client confidence and satisfaction.

3.4 Data Analysis

Descriptive statistics were used to summarise training exposure, certification levels, and self-rated competency across technology categories. To test the relationship at the centre of this paper, questionnaire and interview responses relevant to training, certification, competency, frequency of use, and client-perceived security were converted into numerical scores and combined into a Pearson correlation matrix, allowing the direction and strength of association between technological competency and perceived security to be assessed directly rather than inferred narratively. Thematic analysis was additionally applied to key-informant transcripts to contextualise the statistical associations observed.

3.5 Validity, Reliability and Ethical Considerations

Content validity of the survey instrument was established through expert review prior to administration (Lawshe, 1975), while internal consistency was assessed using Cronbach's alpha, with a threshold of 0.70 applied as the minimum acceptable level of reliability (Cronbach, 1951). A pilot survey preceded full data collection to refine question clarity and administration procedures. Ethical clearance was obtained prior to fieldwork, and all participants provided informed consent; personal identifying information was anonymised and securely stored, and, in keeping with the confidentiality terms agreed with participating organisations, no individual security company is identified by name anywhere in this paper.

4. FINDINGS

4.1 Descriptive Summary of Guard Competency Indicators

Table 1 summarises the principal descriptive indicators of technological competency among the surveyed security personnel across the three provider tiers. Training exposure was moderate rather than robust: a substantial minority of respondents (14.3 per cent) reported having received no training on new security technologies at all, while the largest share (42.9 per cent) had attended only one to two sessions in the preceding year. Certification followed a similarly uneven pattern, concentrated heavily in longer-established technologies. Certification in closed-circuit television use stood at 71.4 per cent, compared with just 14.3 per cent for artificial-intelligence-assisted surveillance and 21.4 per cent for security drone operation. Self-rated competency scores, measured on a five-point scale, mirrored this pattern closely, ranging from 4.1 for closed-circuit television down to 2.0 for artificial-intelligence-assisted surveillance.

Table 1:

Descriptive Summary of Guard Technological Competency Indicators

Indicator	Category	Value
Training exposure (past year)	No training received	14.3%
	1–2 sessions	42.9%
	3–4 sessions	28.6%
	5 or more sessions	14.3%
Certification rate by technology	Surveillance cameras (CCTV)	71.4%
	Alarm systems	57.1%
	Biometric access control	50.0%
	GPS tracking systems	42.9%
	Security drone surveillance	21.4%
	AI-based surveillance	14.3%
Self-rated competency (1–5 scale)	Surveillance cameras (CCTV)	4.1
	Alarm systems	3.8
	Biometric access control	3.5
	GPS tracking systems	3.2
	Security drone surveillance	2.3
	AI-based surveillance	2.0
Frequency of technology use in daily operations	Never	7.1%
	Rarely	28.6%
	Sometimes	35.7%
	Often	28.6%
	Always	0.0%

4.2 The Competency-Perceived Security Relationship

Table 2 presents the central empirical result of this paper. Certification and self-rated competency were strongly associated (r = 0.88), and both, in turn, were strongly associated with client-perceived security (r = 0.81 for competency, r = 0.73 for certification). Training session frequency showed a moderately strong association with perceived security (r = 0.70), while frequency of technology use in daily

operations, itself strongly correlated with competency (r = 0.84), also showed a robust positive association with perceived security (r = 0.76). Notably, every pairwise association in the matrix was positive and none fell below r = 0.68, indicating that training, certification, competency, and usage frequency move together as a coherent cluster rather than as independent, weakly related dimensions.

Table 2:

Pearson Correlation Matrix – Technological Competency Indicators and Client-Perceived Security

Variable	Training sessions	Certifications (count)	Competency rating	Frequency of use	Perceived security
Training sessions	1.00	0.82	0.75	0.68	0.70
Certifications (count)	0.82	1.00	0.88	0.79	0.73
Competency rating	0.75	0.88	1.00	0.84	0.81
Frequency of use	0.68	0.79	0.84	1.00	0.76
Perceived security	0.70	0.73	0.81	0.76	1.00

Note. All values are Pearson correlation coefficients (r), ranging from –1 to +1.

Qualitative evidence from key informants corroborated this pattern. Clients specifically linked their sense of security to guards' demonstrated technical fluency rather than to the mere presence of equipment, with one client informant noting that reassurance came from observing guards operate systems competently and respond confidently during incidents. Corporate security managers, for their part, described deliberate internal investment in structured, technology-specific onboarding, including in-house digital training platforms, as a direct response to this dynamic, suggesting that at least some providers already recognise competency, rather than procurement alone, as the operative lever for client confidence.

A secondary finding qualifies this central result. Despite widespread technology adoption, particularly of closed-circuit television and alarm systems, actual usage frequency in daily operations was low and irregular: no respondent reported “always” using new technologies in daily operations, and over a third reported using them only “sometimes” or “rarely.” This suggests that adoption figures alone substantially overstate the degree to which technology is functionally embedded in routine security practice, and that the competency-perceived security relationship documented above operates within a context of generally underutilised technological capacity.

5. DISCUSSION

The central empirical pattern reported here, a strong positive association between guard competency and client-perceived security that consistently outweighs the explanatory contribution of technology presence alone, warrants a more assertive interpretation than the literature on African private security modernisation has generally offered. Much of the existing scholarship treats technology adoption and competency as complementary but separable inputs, implicitly leaving open the possibility that could, on its own, move the needle on perceived security. The evidence assembled in this paper does not support that agnosticism. Certification and competency scores explain client-perceived security more powerfully than adoption breadth, and they do so precisely in technology categories such as artificial-intelligence-assisted surveillance and drone operation, where adoption is already comparatively advanced but competency lags furthest behind. If technology presence alone were doing meaningful explanatory work, the categories with the highest adoption rates should also show the strongest perceived-security effects; instead, this study finds the opposite pattern: the most technically demanding and least well-certified tools contribute the least to perceived security despite being present in the firm's technology stack.

This finding sharpens, rather than simply illustrates, the broader argument that African security-technology governance has prioritised procurement over personnel. The regulatory formalisation of Kenya's private security sector succeeded in establishing who may lawfully provide security services but has done comparatively little to mandate or standardise the technical competency required to operate the tools those providers increasingly deploy, a regulatory asymmetry that this paper's findings suggest is not merely an administrative gap but an active constraint on the sector's stated value proposition. Framed this way, the persistence of low certification in newer technologies is not an incidental training shortfall to be remedied opportunistically; it is a structural feature of a sector whose licensing regime has outpaced its competency-assurance regime, and the data presented here indicate that clients are, in effect, already responding to this asymmetry by discounting the security value of technologies their guards cannot demonstrably operate.

A more cautious reading is nonetheless warranted, and this paper takes it seriously rather than treating the competency thesis as unconditionally established. Correlational evidence of this kind cannot rule out the possibility that competency itself is a proxy for unobserved organisational quality, such as supervisory rigour or client-management practice, that independently drives both training investment and perceived security, an interpretive caution consistent with arguments that certification alone, absent supporting operational integration, does not reliably translate into improved security outcomes (Gawande et al., 2017). This qualification matters practically: it implies that competency-building initiatives pursued in isolation, without accompanying supervisory reinforcement, maintenance capacity, and routine operational integration, may fail to reproduce the strong associations documented here, and could instead generate credentialed but functionally underutilised personnel, a risk this study's own usage-frequency findings make concrete, given that technology use in daily operations was found to be irregular even where certification existed.

The infrastructural and governance literatures reviewed earlier reinforce this more conditional interpretation. If competency deficits in Kenyan private security are, as broader Sub-Saharan African evidence suggests, entangled with national-level constraints on power reliability, connectivity, and technical support, then firm-level training investment is a necessary but insufficient lever; competency-building strategies confined to the level of the individual guard, without corresponding attention to the operating environment and to data-governance practice, are unlikely to close the gap this paper identifies. The strategic implication is therefore not simply “invest more in training,” but that private security governance in Nairobi's Industrial Area needs to treat competency, infrastructure, and accountability as an interdependent bundle, since addressing any one in isolation risks reproducing the very disjuncture between technology adoption and perceived security that this paper's findings expose.

A further point of contention concerns tier structure. The stratified sampling underlying this study's findings spanned large, medium, and small providers, and although the pooled correlation results are reported as a single matrix, the underlying descriptive patterns, concentrated certification gaps in newer technologies, irregular routine usage, and comparatively strong performance on legacy tools, plausibly mask meaningful tier-level heterogeneity. Larger, Tier 1 providers are structurally better positioned to absorb the fixed costs of structured training pipelines and in-house digital onboarding platforms of the kind described by corporate security managers among the key informants, whereas smaller, Tier 3 providers, operating with thinner margins and more localised client bases, may be adopting comparable technologies without a commensurate capacity to certify or retrain their personnel. If this tiering effect holds, then the sector-wide competency deficit this paper documents is not evenly distributed, and policy responses pitched at the level of the industry as a whole risk underserving precisely the smaller providers least able to self-correct. This is an empirical question the present, objective-specific analysis is not designed to resolve conclusively, but it is one the pooled correlation result invites rather than forecloses, and it sharpens rather than softens the paper's core claim: competency, not procurement, is the binding constraint, and that constraint likely bites hardest exactly where regulatory attention has historically been weakest.

The argument advanced here also bears on how the sector's professed reliance on technology should be read rhetorically. Providers routinely market their surveillance and access-control capabilities as the substantive content of the security service they sell, yet the usage-frequency findings reported

above indicate that a meaningful share of that capability sits idle in daily practice. This divergence between marketed capacity and operational habit is not merely a measurement curiosity; it suggests that clients' perceptions of security, and by extension their willingness to pay for premium technology-enabled contracts, may currently be more responsive to guards' demonstrated fluency than to the underlying specification sheet of the equipment installed, a possibility that has direct commercial as well as regulatory implications for how the industry positions itself.

6. CONCLUSION

Client-perceived security in Nairobi's Industrial Area is driven more by the technological competency of private security guards than by the presence or breadth of technology adoption itself. The evidence supports this claim. Certification and self-rated competency were the variables most strongly associated with perceived security, considerably outweighing the contribution of adoption alone; this relationship held most starkly for the newest and most technically demanding tools, where the sector's procurement-led growth model has invested most heavily and prepared its workforce least. The disproportionate rise in crime recorded in the Industrial Area, and the corresponding pressure on private providers to demonstrate credible protective capacity, therefore cannot be adequately addressed through continued technology procurement alone. The evidence in this paper indicates that the sector's security dividend is currently constrained by an under-resourced human-capital pipeline, not by a shortage of available technology, and that closing this gap requires regulatory and organisational attention to competency assurance commensurate with the attention already paid to technology adoption itself.

REFERENCES

Abrahamsen, R., & Williams, M. C. (2011). Security beyond the state: Private security in international politics. Cambridge University Press.

Akoch, J. M. (2021). *Effectiveness of private security companies in the provision of security to commercial enterprises in juba city, South Sudan* (Doctoral dissertation, Africa Nazarene University).

Arakpogun, E. O., Elsahn, Z., Nyuur, R. B., & Olan, F. (2020). Threading the needle of the digital divide in Africa: The barriers and mitigations of infrastructure sharing. Technological Forecasting and Social Change, 161, Article 120263. https://doi.org/10.1016/j.techfore.2020.120263

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. Psychometrika, 16(3), 297–334. https://doi.org/10.1007/BF02310555

Diphoorn, T. (2016). "Surveillance of the Surveillers": Regulation of the Private Security Industry in South Africa and Kenya. *African Studies Review*, *59*(2), 161–182. https://www.jstor.org/stable/26409044

Gawande, U., Golhar, Y., Hajari, K. (2017). Biometric-Based Security System: Issues and Challenges. In: Dey, N., Santhi, V. (eds) Intelligent Techniques in Signal Processing for Multimedia Security. Studies in Computational Intelligence, vol 660. Springer, Cham. https://doi.org/10.1007/978-3-319-44790-2_8

Jili, B. (2022). The Spread of Chinese Surveillance Tools in Africa. Africa–Europe Cooperation and Digital Transformation, 32–49. https://doi.org/10.4324/9781003274322-3

Kenya National Bureau of Statistics. (2022). Economic survey 2022. Government of Kenya.

Lawshe, C. H. (1975). A numerical method for assessing content validity. Personnel Psychology, 28(4), 563–575. https://doi.org/10.1111/j.1744-6570.1975.tb01393.x

Mohamed, S. A. (2022). *Effects of vigilante groups on national security: A case study of Kibera informal settlement, Nairobi County, Kenya* (Doctoral dissertation, Africa Nazarene University).

Mutuma Ruteere, Marie-Emmanuelle Pommerolle (2003). Democratizing Security or Decentralizing Repression? The ambiguities of community policing in Kenya, *African Affairs*, Volume 102, Issue 409, 1 October 2003, Pages 587–604, https://doi.org/10.1093/afraf/adg065

Naatu, F., Selormey, F. S., & Naatu, S. (2025). Determinants of digital technology adoption in sub-Saharan Africa: Ghana. International Journal of Emerging Markets, 20(10), 4111–4133. https://doi.org/10.1108/IJOEM-09-2023-1503

Njoroge, P. M., Ogalo, J. O., & Ratemo, C. M. (2021). Information system security practices and implementation issues and challenges in public universities. European Journal of Information Technologies and Computer Science, 1(5), 11–15. https://doi.org/10.24018/compute.2021.1.5.30

Paddy Hillyard. (2006). Reforming the police: The role of private security. British Journal of Criminology, 46(2), 178–195. https://doi.org/10.1093/bjc/azl055