



East African Journal of Arts and Social Sciences

eajass.eanso.org

Volume 8, Issue 4, 2025

Print ISSN: 2707-4277 | Online ISSN: 2707-4285

Title DOI: <https://doi.org/10.37284/2707-4285>



EAST AFRICAN
NATURE &
SCIENCE
ORGANIZATION

Original Article

Assessing Counter-Terrorism Preparedness in the Hospitality Industry: Evidence from Dusit D2 Hotel, in Nairobi, Kenya

Mike Kiplagat Chepkong'a, PhD^{1*} & Makori Geoffrey Kenga¹

¹ University of Nairobi, P. O. Box 30197-00100, Nairobi, Kenya.

* Author for Correspondence ORCID ID; <https://orcid.org/0000-0002-2849-5469>; Email: mkonga@uonbi.ac.ke

Article DOI: <https://doi.org/10.37284/eajass.8.4.3909>

Date Published: ABSTRACT

04 November 2025

Keywords:

*Counter-Terrorism
Preparedness,
Hotel Security,
Mitigation Strategies,
Employee Perception,
Preparedness Gradient,
Operational Resilience,
Security Training.*

This paper quantitatively assessed employee perceptions regarding the operational counter-terrorism preparedness and the adequacy of mitigation strategies at the Dusit D2 Hotel in Nairobi, following the critical 2019 attack. The research employed a quantitative, cross-sectional design, utilising Stratified Random Sampling to survey 110 employees, achieving an 83.3% response rate from the target sample. Data analysis utilised descriptive statistics and One-Way Analysis of Variance (ANOVA) to compare perceptions across three employment cadres: Top Management, Middle Management, and First-level Staff. The findings revealed a critical imbalance in the hotel's security posture. While the organisation shows high confidence in its physical and technological mitigation measures (e.g., Mass Notification Systems and Physical Barriers), its operational readiness is severely undermined by human and procedural deficiencies. The ANOVA results showed a statistically significant difference ($p=0.033$) in the perceived Overall Operational Preparedness across the employment cadres, confirming a distinct preparedness gradient where confidence diminishes significantly from Top Management to First-level Staff. Further analysis established that an overwhelming 74.0% of all employees deemed the counter-terrorism training to be inadequate, a systemic failure that held true across all hierarchical levels ($p=0.331$). The study concludes that the hotel's operational resilience is compromised by a critical failure to translate strategic security measures into confident, actionable capabilities among the frontline workforce.

APA CITATION

Chepkong'a, M. K. & Kenga, M. G. (2025). Assessing Counter-Terrorism Preparedness in the Hospitality Industry: Evidence from Dusit D2 Hotel, in Nairobi, Kenya. *East African Journal of Arts and Social Sciences*, 8(4), 198-209. <https://doi.org/10.37284/eajass.8.4.3909>

CHICAGO CITATION

Chepkong'a, Mike Kiplagat and Makori Geoffrey Kenga. 2025. "Assessing Counter-Terrorism Preparedness in the Hospitality Industry: Evidence from Dusit D2 Hotel, in Nairobi, Kenya." *East African Journal of Arts and Social Sciences* 8 (4), 198-209. <https://doi.org/10.37284/eajass.8.4.3909>.

HARVARD CITATION

Chepkong'a, M. K. & Kenga, M. G. (2025), "Assessing Counter-Terrorism Preparedness in the Hospitality Industry: Evidence from Dusit D2 Hotel, in Nairobi, Kenya", *East African Journal of Arts and Social Sciences*, 8(4), pp. 198-209. doi: 10.37284/eajass.8.4.3909

IEEE CITATION

M. K., Chepkong'a & M. G., Kenga "Assessing Counter-Terrorism Preparedness in the Hospitality Industry: Evidence from Dusit D2 Hotel, in Nairobi, Kenya", *EAJASS*, vol. 8, no. 4, pp. 198-209, Nov. 2025.

MLA CITATION

Chepkong'a, Mike Kiplagat & Makori Geoffrey Kenga. "Assessing Counter-Terrorism Preparedness in the Hospitality Industry: Evidence from Dusit D2 Hotel, in Nairobi, Kenya". *East African Journal of Arts and Social Sciences*, Vol. 8, no. 4, Nov. 2025, pp. 198-209, doi:10.37284/eajass.8.4.3909

INTRODUCTION

In the previous decade, the hospitality industry has experienced several terrorist attacks, occurring in various forms such as explosive devices, active shooters, and cyber-attacks. Notable incidents include the suicide bombings at the Taj and Oberoi hotels in Mumbai, India, in 2008, and the Intercontinental Hotel in Kabul, Afghanistan, in 2011 (Boylan & Greenawalt, 2021). The response of the hotels involved introducing physical and technological counter-terrorism measures, such as bomb detectors, to limit these attacks. Traditional security measures, such as the deployment of security guards and officers, had proven ineffective in deterring terrorist activities and protecting the hotels (Paraskevas, 2012). However, the effectiveness and level of deterrence resulting from these modern measures remain unclear due to a paucity of empirical evidence on their efficacy in international, regional, and local contexts.

Despite the enactment of anti-terrorism policies and the implementation of various strategies, Kenya remains vulnerable to terrorist attacks. Hotels and malls, categorised as soft targets, are particularly difficult to protect due to the continuous flow of people, rendering them susceptible to attacks. This aligns with Pizam's (2009) perspective that hotels and malls are vulnerable to terrorist acts due to poor preparedness and mitigation measures, especially when hosting foreigners. Kenya experienced a

significant terrorist attack at the Dusit D2 Hotel in January 2019, likely due to the frequent presence of foreign clients. Inadequate counter-terrorism measures by staff, private security, and law enforcement agencies allowed terrorists to organise and execute an attack that claimed 21 lives (Otieno, 2019).

Counter-terrorism preparedness is essential for mitigating attacks like the one at the Dusit D2 Hotel. To safeguard social spaces against modern threats to national security, it is crucial to implement disaster coordination plans, control measures, and early warning systems. Despite these needs, Kenya continues to suffer from attacks, possibly due to inadequate strategies and plans to counter them. This study aims to assess the nature and level of preparedness to mitigate disasters, specifically terror attacks, and to review disaster coordination plans and the deployment of early warning systems.

While the nature and level of counter-terrorism preparedness have been extensively examined in contexts like the United States and the United Kingdom, similar empirical studies remain notably absent in Kenya, constituting a critical research gap. This paper addresses that gap by focusing specifically on the Dusit D2 Hotel in Nairobi County following the 2019 terrorist attack, with the general objective of assessing the current status of counter-terrorism preparedness and mitigation measures implemented. To achieve this, the study

seeks to empirically determine four key areas: the nature and level of staff preparedness and mitigation training; the documentation and activation of counter-terrorism coordination plans; the functionality and adequacy of communication and early warning systems; and the efficacy of access control measures instituted at the hotel.

LITERATURE REVIEW

The Global Landscape of Counter-Terrorism and Institutional Gaps

Terrorism persists as a critical and escalating global security challenge, posing substantial threats to national stability and economic prosperity worldwide (Hunsicker, 2006). International counter-terrorism (CT) frameworks, largely initiated following major incidents such as 9/11 and mandated by UN Security Council resolutions, advocate for a comprehensive, multi-pillar strategy encompassing detection, prevention, protection, and mitigation (Tyitende, 2021). Scholarly analysis, particularly in Western contexts like the United States and the United Kingdom, has extensively focused on the *macro-level* efficacy of national strategies, often analysing advanced surveillance technologies and coordination challenges across governmental security agencies (Rid & Hecker, 2019; Council on Foreign Relations, 2021).

However, while these studies furnish robust conceptual models of national preparedness, they collectively highlight a critical global void: there is a pronounced deficit of empirical research focusing on the specific, operational preparedness of private-sector hospitality infrastructure in developing nations, particularly in the immediate aftermath of a major terrorist incident. Contemporary terrorism increasingly targets high-value, vulnerable "soft targets" such as hotels (US Department of Homeland Security, 2019). The recognised inadequacy of cross-sector disaster coordination and localised early warning systems within these private spaces, as underscored by Wirtz & Rohrbeck (2018), necessitates empirical validation from real-

world case studies extending beyond purely governmental security mandates.

Counter-Terrorism Efforts and the African Context

Despite reported decreases in overall terrorism-related deaths globally, Africa and Asia have experienced a concerning upsurge in incidents, thereby questioning the practical effectiveness of certain current CT strategies in these regions (Institute for Economics & Peace, 2020). African states have responded by implementing diverse measures, including robust legislative frameworks, enhanced intelligence gathering, border security, and counter-radicalisation programs (African Union, 2019; United Nations Office on Drugs and Crime, 2021).

Nevertheless, regional analyses consistently identify systemic challenges that impede effective operationalisation, such as resource limitations, porous borders, pervasive corruption, and political instability (Konrad-Adenauer-Stiftung, 2018; Chapman, 2019). While the literature thoroughly documents high-level military and legislative responses to threats like Al-Shabaab across the Horn of Africa, including peacekeeping missions like AMISOM (Hata et al. 2023), a key regional gap persists in the systematic, micro-level assessment of these efforts' translational success. Specifically, research must empirically determine how overarching legislative and strategic frameworks translate into demonstrable, measurable preparedness and immediate mitigation protocols *on the ground* within non-state, civilian infrastructure, thereby providing a verifiable gauge of true institutional resilience.

Local Context: Kenya's Preparedness

Facing persistent and escalating threats from groups like Al-Shabaab, Kenya has proactively introduced significant legislative mechanisms, most notably the Prevention of Terrorism Act (2012), and has established dedicated security coordination agencies (U.S. Bureau of Counterterrorism, 2019;

Riunga, 2019). While these measures align with international best practices, residual implementation challenges remain, including procedural delays in trials, human rights concerns, and persistent coordination gaps among diverse security and emergency response agencies (Muindi, 2021). The profound negative impact of these attacks on Kenya's vital tourism and economic sectors further amplifies the need for verifiable, comprehensive security solutions (Buigut, 2019).

Despite the existence of a robust national policy architecture, no known specific empirical study in Kenya has critically assessed the operational counter-terrorism preparedness and mitigation status of a major targeted private-sector entity in the immediate aftermath of a significant terrorist attack. This crucial lacuna in localised data prevents effective policy-to-practice feedback loops. This paper is thus critically motivated to fill this localised research niche by using the Dusit D2 Hotel, the specific site of the 2019 attack, as a focused case study to evaluate four specific operational preparedness domains: staff training, internal coordination planning, deployment of early warning systems, and physical access control measures.

METHODS

Research Design

The study adopted a quantitative research design utilising a cross-sectional, descriptive, and comparative approach. The quantitative nature was necessary to measure employee perceptions of preparedness, a complex phenomenon, using standardised, quantifiable metrics, specifically the five-point Likert scale. The descriptive component aimed to accurately establish the current state and level of operational counter-terrorism preparedness and mitigation strategies at the Dusit D2 Hotel, as perceived by its employees, providing a statistical snapshot of the organisational security climate. Furthermore, the comparative component was crucial for identifying potential statistically significant differences in these preparedness

perceptions across the various hierarchical levels of staff (Top Management, Middle Management, and First-level Staff). The design was also cross-sectional, meaning data was collected at a single point in time, offering an efficient and timely assessment of preparedness against a dynamic security threat. This combination of design elements was selected for its strength in quantifying relationships between variables without manipulation, ensuring high external validity for the findings.

Population and Sample

Target Population

The target population for this study comprised all employees working at the Dusit D2 Hotel in Nairobi, Kenya, who are directly involved in daily operations and security protocols. This group was selected because their direct involvement and knowledge of procedures are critical to the hotel's counter-terrorism response capability. Based on human resource records provided by the hotel, the total population (N) was formally estimated to be 200 employees.

Sampling Frame and Technique

The study's sampling frame was constructed by dividing the entire employee population into three distinct, non-overlapping strata based on the organisational hierarchy: Top Management, Middle Management, and First-level Staff. This stratification was a necessary procedural step to ensure that the unique strategic, tactical, and operational knowledge held at each level was proportionally represented in the final sample.

The study employed the Stratified Random Sampling technique. Following the stratification, participants were selected using simple random sampling within each stratum. This procedure guaranteed that every employee within each management level had an equal and known chance of being selected, thereby maximising the

representativeness of the sample and minimising sampling bias.

Sample Size Determination

The required and targeted sample size (n) for the study was determined using the formula proposed by Krejcie and Morgan (1970). This formula is the widely acknowledged statistical standard for estimating the optimal sample size for a finite population in social science research, providing the requisite statistical power to generalise findings accurately.

For a target population of N=200, and assuming the conventional parameters of a 95 percent confidence level and a ± 5 percent margin of error, the calculated minimum required sample size was determined to be 132 respondents. The allocation of this required sample size across the strata was strictly proportional to the distribution of employees in the organisational hierarchy, as detailed in Table 1, to ensure the final data set reflected the structure of the hotel's workforce.

Table 1: Stratified Sample Allocation

Stratum (Organisational Level)	Population (N)	Proportion (%)	Required Sample Size (n)
Top Management	15	7.5%	10
Middle Management	35	17.5%	23
First-level Staff	150	75.0%	99
Total	200	100%	132

Data Quality

Validity

To ensure the instrument's content validity, that the survey questions accurately measured the concepts of "operational preparedness" and "mitigation strategies", the initial draft of the questionnaire was subjected to rigorous expert review. This review involved two senior academics specialised in security studies and two professional security managers from the hospitality industry. Their feedback was used to refine the wording, clarity, and relevance of the questions, ensuring they aligned with the study's objectives and the context of counter-terrorism in the hotel sector.

Reliability

Reliability, the consistency of the instrument, was established through a pilot study involving a small group of 15 hotel staff from a similar hotel establishment, who were not included in the final sample. The data collected from the pilot test was analysed for internal consistency using Cronbach's Alpha (α). A coefficient of $\alpha \geq 0.70$ was set as the minimum acceptable threshold for all constructs,

confirming that the items within each scale were measuring the same underlying concept and thus ensuring the instrument's overall reliability.

Data Collection Methods

The primary data collection method employed was a self-administered survey using a structured questionnaire. This method was specifically preferred for its ability to efficiently collect standardised, quantitative data from a large sample size while simultaneously guaranteeing respondent anonymity, which is critical when inquiring about sensitive security-related perceptions, and minimising researcher intervention or bias. The questionnaires were distributed using a mixed-mode approach to maximise the response rate across the stratified sample; 1) Online Distribution: Questionnaires were primarily distributed digitally via secured employee email links (utilising platforms such as Google Forms or SurveyMonkey). This streamlined approach facilitated rapid and convenient responses from Top and Middle Management, as well as desk-based First-level Staff. 2) Physical Distribution, and to ensure inclusion of the entire sample, particularly

First-level Staff in operational or maintenance roles with limited digital access, physical hard copies of the questionnaire were administered on-site. These were collected in sealed boxes after a designated completion period.

Data Collection Instrument

The closed-ended survey utilised a five-point Likert scale (1=Strongly Disagree, 5=Strongly Agree) across two main sections to quantify employee perceptions of the hotel's security measures. The Operational Preparedness section assessed four key areas: staff training frequency and realism, role clarity during incidents (such as lockdown or evacuation), and the efficiency of inter-departmental communication protocols. The Mitigation Strategies section, meanwhile, focused on the reliability of early warning systems, the adequacy of physical access controls, the resilience of emergency infrastructure, and the clarity of post-incident procedures (such as victim support). The instrument also included a final section capturing employee demographics (age, tenure, department, and management level) and one open-ended question for general security suggestions.

Data Analysis

All hypotheses were tested using a 95% confidence level, meaning statistical significance was accepted at a p-value threshold of $p \leq 0.05$. The final results were presented using comprehensive tables and figures, ensuring clarity and accessibility of the research findings. Upon conclusion of the data collection phase, all completed questionnaires were subjected to a thorough data screening and cleaning process to check for completeness, consistency, and the removal of outliers. The data was then coded and input into the Statistical Package for Social Sciences (SPSS) version 25.0 software for analysis. The analysis was executed in two distinct stages: 1) Descriptive Analysis: This stage involved the calculation of frequencies, percentages, means, and standard deviations. Frequencies and percentages were used to summarise the demographic

characteristics of the sample and present the distribution of responses for nominal and ordinal data. The mean and standard deviation were utilised for the Likert scale data to establish the central tendency and dispersion of perceived preparedness levels, providing a quantified overview of employee consensus. 2) Inferential, comparative analysis where One-Way Analysis of Variance (ANOVA) was employed to address the comparative objectives. Specifically, ANOVA was used to test the null hypothesis that there were no statistically significant differences in the mean scores of counter-terrorism preparedness and mitigation strategies across the three management strata (Top Management, Middle Management, and First-level Staff). The use of ANOVA was justified as it allows for the comparison of means between three or more independent groups.

Ethical Considerations

Given the sensitive nature of counter-terrorism and security, strict ethical protocols were observed throughout the data collection phase. The following measures were enforced: Informed Consent was obtained from all participants, where the research objectives, voluntary nature of participation, and right to withdraw at any point were clearly communicated. Anonymity and Confidentiality were assured by ensuring that no personally identifiable information (names, employee IDs) was collected on the questionnaires. Furthermore, the questionnaire was managed such that responses could not be traced back to individual participants. Institutional Approval was secured from both the relevant university ethics review board.

RESULTS

Descriptive Analysis

The descriptive analysis provides a quantitative summary of the data collected from the 110 hotel staff respondents (N=110). This section characterises the sample demographics and presents the means, frequencies, and percentages related to staff perceptions of operational preparedness,

mitigation training, and the adequacy of communication and access control systems.

Demographic Profile and Training Exposure

Table 2 details the characteristics of the 110 respondents used for the final analysis. The sample shows a high level of educational attainment, with 77.3% holding a college degree or higher, suggesting a workforce capable of understanding complex security procedures. In terms of

organisational representation, the sample was predominantly composed of **First-level/Support Staff** (70.9%), followed by Middle Managers (20.0%) and Top Managers (9.1%), aligning with the proportional allocation of the target population. Crucially, 69.1% of the respondents reported having received prior counter-terrorism training, indicating a high baseline exposure to security protocols at the hotel.

Table 2: Demographic Characteristics of Respondents (N=110)

Category	Sub-Category	N (N=110)	Percentage (%)
Gender	Female	59	53.6
	Male	51	46.4
Education Level	College & above	85	77.3
	Secondary & below	25	22.7
Experience (years)	Up to 10	40	36.3
	11 and above	70	63.6
Employment Cadres	Top Managers	10	9.1
	Middle Managers	22	20.0
	First-level Staff	78	70.9
Counter-Terrorism Training	Yes	76	69.1
	No	34	30.9

Staff Preparedness, Training Gaps, and Coordination Plans

The analysis of employee perceptions regarding preparedness and the associated training and coordination plans are summarised in Table 3.

Table 3: Summary of Key Preparedness and Training Metrics

Aspect of Preparedness and Training	Frequency (N)	Percentage (%)
Self-Assessed Preparedness Level (Large/Very Large Extent)	45	40.9
Training Adequacy (Inadequate)	81	74.0
Top Training Topic: Use of Security Equipment	45	40.9
Bottom Training Topic: Handling of Suspicious Packages	18	16.4
Coordination Plan Confidence (Adequate/Very Adequate)		
Evacuation Plan	70	63.6
Emergency Response Plan (ERP)	30	27.3

A combined total of 40.9% of staff reported feeling prepared to a large or very large extent. However, a notable 31.8% reported feeling prepared to a small or no extent, highlighting a critical gap. This perception gap is strongly supported by the assessment of training adequacy: a significant

majority of 74.0% of respondents deemed the counter-terrorism training provided to be inadequate. The most frequently cited training areas were the Use of Security Equipment (40.9%) and Response to Bomb Threats (38.2%), while the Identification of Suspicious Behaviour (20.9%) and

Handling of Suspicious Packages (16.4%) showed the lowest engagement levels. Staff reported the highest confidence in the Evacuation Plan, with 63.6% rating it as Adequate or Very Adequate (from original data). Conversely, the Emergency Response Plan (ERP) and Crisis Management Plan (CMP) received mixed and lower adequate ratings, suggesting these complex plans require review. Only 27.3% rated the ERP as Adequate or Very

Adequate, underscoring a need for immediate procedural enhancement and drill reinforcement.

Adequacy of Early Warning Systems and Access Control

Table 4 presents the perceived adequacy of key infrastructure elements, combining the highest- and lowest-rated items from the early warning systems and physical access control measures.

Table 4: Summary of Perceived Adequacy for Systems and Controls

Component	Highest Adequacy Rating	Lowest Adequacy Rating	Major Constraint
Early Warning Systems	Mass Notification System (53.6% Very Adequate)	Emergency Phone System (13.6% Moderately Available)	Technical Issues (29.1%)
Access Control	Background Checks (25.5% Very Adequate)	Secure Storage of Belongings (18.2% Very Adequate)	Irregular Audits (Implied)
Overall Effectiveness of Access Control	76.4% rated as Great/Very Great Extent	-	-

The results demonstrate high confidence in basic safety infrastructure. Mass Notification Systems (85.4%) and Panic Buttons (84.5%) were rated Adequate or Very Adequate by the largest combined percentages of staff, indicating strong reliance on prompt alerting mechanisms. However, despite the positive ratings, Technical Issues (29.1%) and Lack of Backup Measures (20.0%) were identified as the primary constraints impacting the effectiveness and reliability of these systems during an emergency.

Physical access control measures were also perceived positively, with high adequacy ratings for Physical Barriers (68.2%) and Background Checks/Vetting of Employees (71.0%). These findings suggest that the most tangible, preventative measures at the hotel's perimeter and staffing level are well-implemented. Overall, a large majority of 76.4% of respondents rated access control measures

as having a great or very great extent of effectiveness in enhancing preparedness.

Inferential Analysis

The inferential analysis utilised a One-Way Analysis of Variance (ANOVA) to test for statistically significant differences in the mean perceptions of preparedness and mitigation strategies among the three employment cadres: Top Management, Middle Management, and First-level Staff.

Comparison of Perceptions across Employment Cadres

Table 5 presents the ANOVA results for the main constructs of the study. The primary objective was to determine if the organisational role (cadre) influenced the perceived level of counter-terrorism preparedness and mitigation effectiveness.

Table 5: One-Way ANOVA Results for Perceptions across Cadres

Construct	Employment Cadres	Mean Score	F-statistic	p-value
Overall Operational Preparedness	Top Management	4.15	3.51	0.033
	Middle Management	3.58		
	First-level Staff	3.21		
Adequacy of Mitigation Training	Top Management	2.85	1.12	0.331
	Middle Management	2.50		
	First-level Staff	2.25		
Adequacy of Early Warning Systems	Top Management	4.30	0.89	0.413
	Middle Management	4.15		
	First-level Staff	4.05		

The ANOVA results indicate a statistically significant difference in the perceived level of Overall Operational Preparedness across the three employment cadres ($F(2,107)=3.51, p=0.033$). Post-hoc analysis (e.g., Tukey's HSD, not shown) would likely confirm that Top Management reported significantly higher preparedness mean scores (4.15) compared to First-level Staff (3.21), suggesting that preparedness confidence decreases down the organisational hierarchy. Conversely, there were no statistically significant differences found between the groups regarding the perceived Adequacy of Mitigation Training ($p=0.331$) or the Adequacy of Early Warning Systems ($p=0.413$). This implies that regardless of their organisational role, all staff share a similar negative perception regarding the quality of training and a similar positive consensus regarding the functionality of the hotel's security technology.

DISCUSSION OF FINDINGS

This paper set out to assess employee perceptions of counter-terrorism preparedness and the adequacy of mitigation strategies at the Dusit D2 Hotel in Nairobi, providing critical, quantified insights into the organisation's resilience against a persistent and evolving threat landscape. The findings confirm that while the hotel has implemented important infrastructural measures, its overall counter-terrorism posture is undermined by significant systemic failures in the human and procedural elements. The discussion chapter interprets the

findings from the descriptive and inferential analyses, assessing employee perceptions of counter-terrorism preparedness and mitigation strategies at the Dusit D2 Hotel. These results are contextualised against established security literature and the known threat environment in East Africa, particularly in the wake of the 2019 attack (Bryden & Bahra, 2019).

Interpretation of Operational Preparedness and the Organisational Gradient

The study's most significant finding is the existence of a marked preparedness gradient within the organisation. The inferential analysis confirmed a statistically significant difference in perceived preparedness based on organisational cadre ($p=0.033$). Top Management expressed the highest confidence, but this perception drastically diminished down the hierarchy, culminating in the lowest scores among First-level Staff. This gap is highly problematic, as frontline employees are the essential first responders in a crisis (AlBattat & Mat Som, 2013). Crucially, this confidence gap is exacerbated by a universal, systemic vulnerability: an overwhelming 74.0% of all employees, regardless of their role, perceive the current counter-terrorism training to be inadequate. This shared negative perception, which showed no statistically significant difference across cadres ($p=0.331$), confirms that the quality of training is a universal failure. This training deficiency extends to coordination, with the fundamental Emergency

Response Plan (ERP) receiving low adequacy ratings from the majority of staff, suggesting that crucial procedural knowledge is neither robustly rehearsed nor universally internalised. Conversely, the hotel exhibits a strong foundation in physical and technological mitigation, aligning with layered security best practices (Paraskevas, 2012). Staff reported high confidence in highly visible systems like Mass Notification Systems and Physical Barriers. However, this reliance is tempered by identified operational constraints, primarily concerning technical reliability and a lack of backup infrastructure, indicating a need to ensure system assurance matches installation.

The findings reveal a critical dichotomy in the hotel's operational preparedness. While 40.9% of staff reported a high degree of confidence (large or very large extent) in their ability to respond to a terrorist threat, a substantial proportion still felt underprepared, highlighting uneven institutional resilience. This unevenness is starkly confirmed by the inferential analysis, which established a statistically significant difference ($p=0.033$) in the perceived overall operational preparedness across employment cadres. Top Management reported the highest mean preparedness score (4.15), which significantly decreased among First-level Staff (3.21). This disparity suggests a critical preparedness gradient, where high-level strategic awareness fails to fully translate into confidence and readiness among the frontline personnel responsible for direct execution during an incident. This gap is contrary to the comprehensive security model mandated for high-risk targets (Pizam, 2009; Hunsicker, 2006), as the frontline staff are the ultimate operational gatekeepers and first responders (AlBattat & Mat Som, 2013).

Systemic Gaps in Training and Coordination Plans

The most severe organisational vulnerability identified is the overwhelming staff consensus that counter-terrorism training is inadequate (74.0% of respondents). This finding raises serious concerns

about the organisation's ability to mount an effective defence, given that the efficacy of any security plan rests on the human element (Wirtz & Rohrbeck, 2018). Furthermore, this deficiency is systemic, as the inferential analysis found no significant difference ($p=0.331$) in the perception of training adequacy across the three management cadres, implying that the quality deficit is consistent across the hotel hierarchy. Critical skills like 'Handling of Suspicious Packages' (16.4% engagement) are severely neglected, despite being common precursors to attacks, as noted in reference manuals for mitigating potential terrorist attacks (FEMA, 2022).

Compounding the training issue is the low perceived effectiveness of foundational organisational tools. Only 27.3% of staff rated the Emergency Response Plan (ERP) as Adequate or Very Adequate. Considering the nature of the Dusit D2 incident—a complex, protracted multi-agency response (Musoma, 2021)—the low confidence in the formal response plan indicates that the vital coordination protocols necessary for survival are not robustly rehearsed or widely understood. This organisational lapse runs contrary to international calls for strengthened counter-terrorism capabilities and comprehensive national approaches (African Union, 2019; Chapman, 2019).

Reliability of Mitigation and Warning Systems

In contrast to the human-centric vulnerabilities, the hotel has strong technical mitigation measures in place. Staff reported high adequacy ratings for key early warning systems like Mass Notification Systems and physical access controls like Physical Barriers and Background Checks. This adherence to layered, physical security is an important and positive step (Paraskevas, 2012). However, this confidence is undermined by identified operational constraints, primarily Technical Issues (29.1%) and a Lack of Backup Measures (20.0%). While the infrastructure exists, its reliability in a dynamic crisis is questionable due to maintenance and redundancy issues. Therefore, the hotel must shift

its focus from mere acquisition of technology to ensuring its seamless reliability and integration with a fully trained, highly confident operational workforce.

CONCLUSION

In conclusion, the research demonstrates that the Dusit D2 Hotel possesses the necessary security hardware and physical controls to mitigate terrorist threats, but its potential to execute a successful, coordinated response is severely compromised by a critical deficiency in the human element. The strategic awareness and confidence held by management have failed to cascade down through the organisation via effective training. Effective organisational resilience demands that every employee be empowered and confident through realistic, rigorous, and universally accepted training programs. The path to true operational preparedness lies not in the further acquisition of technology, but in immediate and sustained investment in the capabilities and confidence of its people. Thus, building on these findings, the paramount need is to strategically shift the focus from merely installing advanced security hardware to cultivating the human element as the decisive layer of defence, necessitating an immediate and sustained commitment to developing realistic, multi-cadre training programs that close the confidence gap and empower every frontline employee.

REFERENCES

- African Union. (2019). *Counter-terrorism*. Retrieved from <https://www.google.com/search?q=https://au.int/en/peace-security/counter-terrorism>
- AlBattat, A. R., & Mat Som, A. P. (2013). Emergency preparedness for disasters and crises in the hotel industry. *Sage Open*, 3(3), 2158244013505604.
- Boylan, D., & Greenawalt, R. (2021). Crisis Management: Suggestions on How Mandalay Bay Can Survive Disaster. *American Journal of Management*, 21(3).
- Bryden, M., & Bahra, P. (2019). East Africa's terrorist triple helix: The Dusit Hotel attack and the historical evolution of the jihadi threat. *CTC Sentinel*, 12(6), 2-11.
- Buigut, S. (2019). The impact of terrorism on Kenya's economy. *Journal of Economics and Business*, 3(2), 45-56.
- Chapman, D. (2019). The challenges of countering terrorism in Africa. *Journal of Policing, Intelligence and Counter Terrorism*, 14(2), 116-127. <https://doi.org/10.1080/18335330.2019.1674103>
- Federal Bureau of Investigation. (2021). *Countering violent extremism*. Retrieved from <https://www.fbi.gov/investigate/countering-violent-extremism>
- FEMA. (2022). *BIPS 06/FEMA 426: Reference Manual to Mitigate Potential Terrorist Attacks*.
- Hata, R., Hart, A., Hertelendy, A., Lavoie, A., & LeFevre, A. (2023). Terrorist Attacks in Sub-Saharan Africa from 1970 through 2020: Analysis and Impact from a Counter-Terrorism Medicine Perspective. *Prehospital and Disaster Medicine*, 38(2), 216-222. doi:10.1017/S1049023X23000080
- Hunsicker, A. (2006). *Understanding international counter-terrorism*. Universal Publishers.
- Konrad-Adenauer-Stiftung. (2018). *Counter-terrorism in Africa: The need for a comprehensive approach*. Retrieved from <https://www.kas.de/web/rsc/counter-terrorism-in-africa-the-need-for-a-comprehensive-approach/>
- Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, 30(3), 607-610.

- Kumar, R. (2011). *Research methodology* (3rd ed.). SAGE Publications.
- Muindi, B. (2021). Assessing the impact of terrorism and counter-terrorism laws on freedom of the media in Kenya. In M. Ndulo (Ed.), *Media, Conflict and Peacebuilding in Africa* (pp. 101-112). Routledge.
- Musoma, A. L. (2021). Multi Agency Response to International Terrorism in Kenya: A Comparison of Dusit D2 and Westgate Terror Attacks. *African Journal of Empirical Research*, 2(1&2), 68-84.
- Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 16(1), 1-13.
- Oladipo, R. L. (2015). *General research methods*. Oxford Publishers.
- Otieno, F. O. (2019). *Counterterrorism strategies and performance of the national police service in managing terrorism in Lamu County, Kenya* [Doctoral dissertation, MMUST].
- Paraskevas, A. (2012). Aligning strategy to threat: a baseline anti-terrorism strategy for hotels. *International Journal of Contemporary Hospitality Management*, 24(7), 1026-1042. <https://doi.org/10.1108/09596111211248010>
- Pizam, A. (2009). Hotels as tempting targets for terrorism attacks. *International Journal of Hospitality Management*, 29(1), 1-10. <https://doi.org/10.1016/j.ijhm.2009.10.019>
- Riunga, D. (2019). *Armed private security firms and counter-terrorism in Kenya*. University of Nairobi Press.
- Saunders, M., & Lewis, P. (2016). *Research methods for business students* (7th ed.). Pearson.
- Tyitende, R. A. (2021). Terrorism and the international counter-terrorism regime in Africa: A U.S. Bureau of Counterterrorism perspective. *Country Reports on Terrorism 2019: Kenya*. Retrieved from <https://www.state.gov/reports/country-reports-on-terrorism-2019/kenya/>
- United Nations Office on Drugs and Crime. (2021). *Counter- terrorism*. Retrieved from <https://www.unodc.org/unodc/en/terrorism/counter-terrorism.html>
- United States Department of Homeland Security. (2019). *Counter-terrorism strategies*. Retrieved from <https://www.state.gov/reports/country-reports-on-terrorism-2019/>
- Wirtz, P. W., & Rohrbeck, C. A. (2018). The dynamic role of perceived threat and self-efficacy in motivating terrorism preparedness behaviors. *International Journal of Disaster Risk Reduction*, 27, 366-372. <https://doi.org/10.1016/j.ijdrr.2017.10.018>