Ethiopian Journal of Police Studies (EJPoS): Volume 2 Issue I, November 2026

ISSN (electronic):137-2635

Exploring the Implementation and Effectiveness of Physical Security Measures at the University of Gondar, Ethiopia

Tilahun Gedefaw Fetene[1] and Aragaw Sergo Alem[2*]

Abstract

Physical security management in higher education institutions involves protecting personnel, assets, and information from threats such as theft and vandalism through measures like access control, security personnel, and surveillance. However, various challenges often hinder its effectiveness. Using a mixed-methods research approach and a descriptive research design, the study evaluates the practices and challenges of physical security management at the University of Gondar, Ethiopia. The study surveyed a randomly selected 239 academic and administrative staff, security personnel, and students. It also purposively identified and interviewed 10 key informants, along with document analysis and observation. The study employed descriptive statistics and thematic analysis. The findings reveal that the practice of physical security is less efficient. It also shows that security personnel deployment remains the only relatively strong practice, while critical infrastructure elements such as closed-circuit television (CCTV) surveillance, perimeter fencing, access control systems, and fire safety equipment are inadequate. The major challenges of security management were identified as outdated and non-functional technology, insufficient and stagnant funding, inadequate staffing and training, security infrastructure that failed to keep pace with institutional expansion, and poor inter-agency coordination. Thus, integrating modern security technologies, dedicating increased budgets, standardising enforcement procedures, conducting a comprehensive security audit, investing in capacity building, applying crime prevention through environmental design (CPTED) principles in campus development, launching security awareness campaigns, and advocating for supportive national policies were recommended to improve the security practice at the university.

Keywords: Physical security management, security practice, security challenge, security measures, University of Gondar

DOI: 10.63990/ejpos.v2il.13943.

---

[1] Legal Service & Grievance Handling Unit, Central Gondar Zone Police, Amhara Regional State, Gondar, Ethiopia

[2]*Corresponding author: Research Institute, Ethiopian Police University, email: sergoalem@gmail.com, Cell Phone: +251912747332 P.O. Box: 1503/Sendafa, Ethiopia

This work is licensed to the publisher under the Creative Commons Attribution-Non Commercial-No Derives License.

Introduction

Physical security is a critical aspect of institutional management that protects assets, personnel, and information from damage, theft, fraud, and other physical threats (Landucci et al., 2020). Higher education institutions worldwide face a growing number of complex and varied security concerns (Alexei, 2021). Rapid technological development, climate change, globalization, and unstable geopolitical conditions have all contributed to the emergence of dangers from a variety of frequently unexpected sources (Bács, 2022). Higher education institutions are vulnerable to different security threats such as vandalism, theft, fraud, unauthorized access, public order disturbances, and serious criminal acts (Ekpoh, Edet, & Ukpong, 2020). In higher education institutions, physical security is critical to ensuring the safety of personnel, infrastructure, and information (Pacapac, 2022).

Ineffective physical security can lead to disruption of academic activities, damage to institutional reputation, financial losses, and compromise the safety and well-being of the university community in general (Riskhan, 2024). In contrary, effective physical security can protect assets, safeguard personnel, and prevent financial losses in higher education institutions (Fennelly, 2016). It is important to explore how higher education institutions can implement physical security practices that prioritize the well-being of academic staff, students, and the whole community while minimizing threats (Pacapac, 2022). Less emphasis on physical security can lead to overwhelming consequences, such as financial losses, reputational damage, and even loss of life (Coole & Brooks, 2021). Organizational physical security involves integrating perimeter security, access control, surveillance technologies, and security personnel (Coole & Brooks, 2021).

Higher education institutions are perceived as open and accessible, seen as institutions that promote democracy, welcomed diverse perspectives, and are public resources for inquiry and community engagement (Hadidane & Khelalfa, 2023). The rapid expansion of infrastructure, increasing numbers of students, growing societal challenges, and potential resource constraints can all affect existing security systems and protocols (Ekpoh et al., 2020).

There are also works outlining the general encounters faced by security sectors in higher education, especially in developing countries (Bacs, 2022). However, specific and significant practical assessments of the combined physical security practice—such as how personnel,

technology, and policy are currently combined and their related challenges are limited. The institutions face specific challenges, particularly given their socio-political environment and resource realities (Mishra & Paney, 2024). Most of the existing studies, for instance, Bacs (2022), have focused on theoretical, global, or isolated aspects of security practice, such as technology effectiveness and security personnel training in general. This indicates that few studies have conducted holistic, context-based assessments of how higher education institutions, such as the University of Gondar, manage physical security in practice. There are also gaps in identifying institution-specific weaknesses and evaluating stakeholders' awareness of the effectiveness of existing security measures. Therefore, the purpose of this research is to fill the critical gaps on the physical security of higher education and offer guidance on how higher education institutions can improve their physical security management by providing a clear, empirical analysis, and offering actionable insights to security management.

Thus, the study address the following basic questions: What are the current physical security practices employed to safeguard assets and personnel? How effective are the existing physical security measures in safeguarding the university assets and personnel? What are the key challenges and vulnerabilities in the university's physical security management system? The study, therefore, identifies the challenges encountered in their implementation, and provides important awareness that can contribute to improving the overall security of the University of Gondar.

Conceptualizing Physical Security Management

Physical security management refers to critical discipline concerned with the protection of assets such as people, property, information, and reputation from physical threats. Physical security is a fundamental concept that refers to the state of being free from danger, threat, or harm (Masum & Training, 2024). It includes the measures, strategies, and systems applied to protect individuals, organizations, and assets from potential risks or vulnerabilities (Masum & Training, 2024). It includes a variety of measures, procedures, and technologies designed to prevent, identify, interrupt, and respond to unauthorized access, theft, vandalism, terrorism, natural disasters, and other adverse events (Onuorah, Eziamaka, & Nonye, 2020). Physical security management incorporates basic elements like integration, layered defense, risk assessment, and taking proactive and reactive measures (Masum & Training, 2024). According

to Karatas (2021) modern physical security management emphasizes proactive measures like deterrence and prevention through environmental design and intelligence processes.

Ekpoh et al. (2020) suggested that higher education institutions present unique security challenges compared with other organizations due to their distinctive working environment. Higher education institutions (HEIs) typically refer to accessible for all or open campuses that promote accessibility, intellectual freedom, and community engagement (Boateng, 2020). A diverse population includes a large, transient group of students, faculty, administrative staff, visitors, contractors, and members of the surrounding community, and this diversity affects access control and identity management (Dar, 2022). Beyond general crime, HEIs can be particularly vulnerable to student protests (which can sometimes escalate), cyber-physical attacks on critical infrastructure, and incidents requiring emergency response for a large, dispersed population (Nuamah, 2025).

This study is grounded in routine activities theory (RAT), the crime prevention through environmental design (CPTED), risk management theory (RMT), systems theory (ST) institutional theory (IT) and human factor theory (HFT) to comprehensively examine the practices and challenges of physical security management at University of Gondar.

The routine activities theory (RAT) suggests that fluctuations in the structure of the patterns of daily activity could explain the rise in crime that occurred (Sasse, 2005). It suggests that crime occurs when three elements occurs in time and space. These are motivated offender an individual with the intent and capability to commit a crime, suitable target persons or objects that is attractive and vulnerable to the offender, and the absence of capable security personnel's the lack of anyone or anything that could prevent the crime, such as a law enforcement officer, witness, or even security system (Steinmetz, 2025).

The crime prevention through environmental design (CPTED) is a crime prevention strategy that focuses on reducing crime and enhancing security through the design and management of the physical environment (Clancey & Fisher, 2016). This theory is relevant to study physical security in higher education institutions because it provides framework for understanding how the design and layout of a facility a given institution can impact its vulnerability to threats. The principles of CPTED include natural surveillance, which indicates designing environments to maximize monitoring and visibility, such as lighting, complete the strategic settlement of windows, and surveillance cameras (Wen et al., 2025).

Risk management theory (RMT) is a framework that focuses on identifying, assessing, and mitigating risks to minimize their impact on an organization (Aven, 2015). RMT involves systematic processes to understand potential threats, evaluate their likelihood and consequences, and implement strategies such as risk avoidance, reduction, transfer, or acceptance (Jonek-Kowalska, 2022).

Systems theory refers to theoretical framework that suggests the component parts of a system can best be understood in the context of the relationships with each other and with other systems (Harney, 2024). By considering the wider context and interconnectedness, security professionals can design more effective and strong solutions for physical security measures (Ahmad et al., 2023). Rather than focusing on individual security devices like cameras or alarms, it needs considering the entire system to apply system theory on physical security managements.

Institutional theory (IT) for physical security emphasizes how organizational practices, structures, and policies related to security are influenced by social norms, regulations, and industry standards (DiMaggio & Powell, 1983). It suggests that organizations adopt certain security measures not only for practical protection but also to conform to expectations, gain legitimacy, and ensure compliance with legal and regulatory requirements.

Human factor theory (HFT) in the context of physical security emphasizes the critical role that human behavior, decision-making, and psychology play in the effectiveness of security measures. It recognizes that vulnerabilities often arise from human errors, negligence, or deliberate malicious actions, making it essential to understand and address human factors in security planning (Reason, 1990).

Based on the basic concepts of these theories, the authors have developed the following

(Figure 1) conceptual framework.

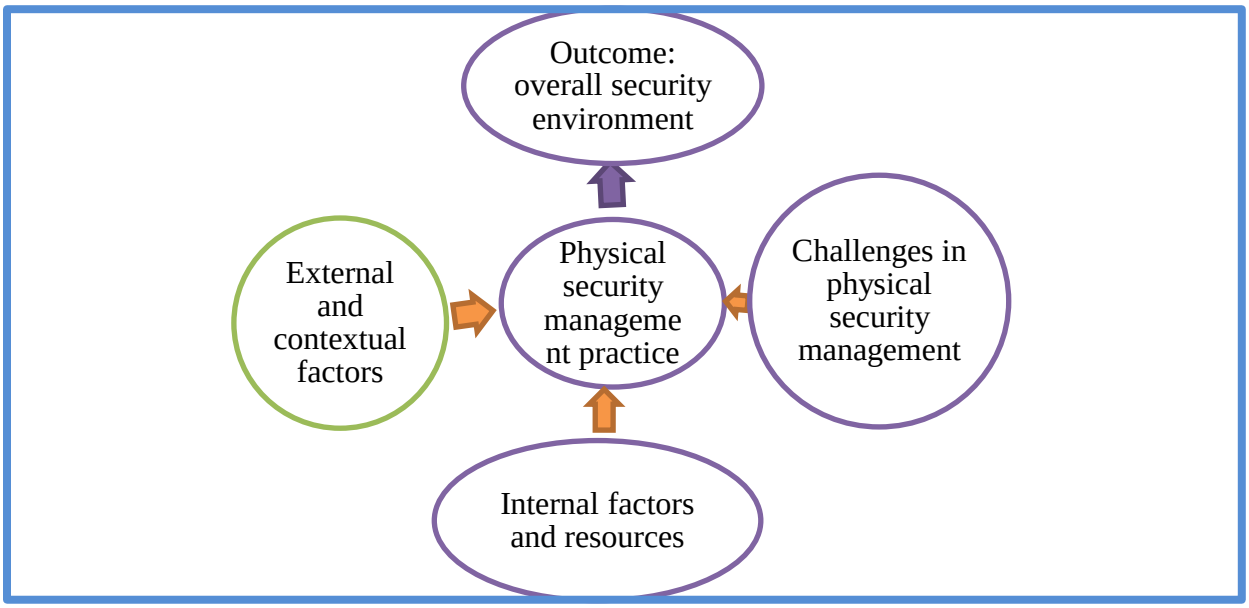

Figure 1: Visual Representation of the Conceptual Framework

As shown in the diagram above, effective physical organizational security practices such as perimeter, access control, surveillance, security personnel, and emergency response contribute to positive organizational outcomes such as asset protection, personnel safety, operational continuity, reputational risk mitigation, and customer confidence.

Materials and Methods

Description of the Study Area

The University of Gondar (UoG), established in 1954 in Gondar, Ethiopia, is one of the largest and a leading public higher education institution. Originating from the Public Health College, it became a university in 2004. UoG has multiple campuses, including Tewodros, Maraki, and Fasil, and is among the largest in Ethiopia. It has played a key role in developing professionals and promoting national progress through education, research, and community service (Alemie & Belaye, 2018).

Using a pragmatic lens the study employed mixed-methods design to comprehensively examine the practices and challenges of physical security management. Both qualitative and quantitative research approach allows for comprehensive understanding of the complex phenomenon of physical security management by triangulating data from different sources and methods, including both primary and secondary data, to empower individuals to share their stories, hear their voices and minimize the power relationships that often exist between the

researchers and the participants in a study (Taherdoost, 2022). Using a mixed-methods approach, the authors was able to gain a deeper understanding of the university's security context.

The target population for this study was security personnel, administrative staff, academic staff, and students of UoG. The data sources were both primary and secondary sources. The primary data were collected from security personnel, administrative staff, and students who are directly and indirectly involved and have more experience with the issue. Structured questionnaires, key informant interviews, and direct observation were employed to collect the primary data. Secondary data were collected from documents such as security policies, organizational charts, incident reports, and previous audit reports from within the past five years.

Data Collection Method, Sampling Techniques and Sample Size

Purposive sampling was used to select key informants such as the head of the security department, security supervisors, deans of key administrative units, representatives from the student council and faculty members. Observation was also conducted to obtain real evidence about physical security management. Thus, actual observation was conducted to collect detailed and insightful physical security practices. The observation questions focused on whether emergency exits are clearly marked, whether biometric scanners are functioning correctly, whether visitor signage is clear and easy to understand, whether surveillance cameras clearly cover the required areas, and whether metal detectors and fire extinguishers are available.

For the quantitative data, the study employed stratified random sampling. Students were stratified by college/department and year of study to ensure adequate representation. Security personnel, academic staff, and administrative staff with more than three years of experience at the University of Gondar were also selected. Employees with less than three years of experience were excluded because they were presumed to have insufficient knowledge of the university's security system. Similarly, only students in their third year or above were included, as they were considered more familiar with security issues at the University of Gondar. First- and second-year students were excluded because of their limited experience with these issues. The sample size for the survey was 254 individuals selected from security Personnel (120), academic and administrative staff (160), and students (410). The sample size was calculated using Yemane's formula as follow.

$n = \frac{N}{1+N((e^{2}))}$ where n= sample size

N=number of population = 690

Therefore, $n = \frac{690}{1+690((0.05)^2)} = 254$

Using the proportional allocation (stratified sampling); the number of samples from each group is distributed as follows (Table 1):

Table 1: Proportional distribution of sample size of the study

Respondent Category	Population	Proportion (%)	Calculated Sample Size	Rounded Sample	Actual numbers of participants
Security Personnel	120	17.4%	254 × 17.4% = 44.2	44	42
Academic & Administrative Staff	160	23.2%	254 × 23.2% = 58.9	59 (30 Academic + 29 Administrative)	55(28 Academic +27 Admin)
Students	410	59.4%	254 × 59.4% = 150.9	151	142
Total	690	100%	254	254	239

As shown in Table 1, the total sample taken from the general population was 254; however, the actual number of participants was 239 due to non-response and their unwillingness to participate in the study. For the qualitative data, 10 individuals were purposively selected: 3 from security personnel, 3 from Academic and Administrative Staff leaders, and 4 from student representatives.

After collecting data through open-ended questionnaires, interviews, and document analysis, the qualitative data is analysed by categorising it thematically according to the research question. The notes taken during the data collection process were translated and contextualised. The translated and contextualized data were organized based on the pre-identified themes. The major themes were organized based on the research objectives. Emerging themes were also integrated into the pre-identified themes. The basic themes identified include physical security practices, physical security measures and the key challenges and vulnerabilities in the

university's physical security management system. Then, the qualitative data collected was transcribed, coded, categorized and interpreted thematically.

Quantitative data were analyzed using frequency and simple percentage descriptions to address the research objectives, and this analysis was supplemented by data obtained through qualitative methods. Multiple strategies were employed to ensure the validity and reliability of the data collected in this study. The instruments were pre-tested with a small group of participants from the head office to identify and resolve ambiguities or inconsistencies, thereby improving their accuracy in capturing the intended information. All participants received consistent instructions and identical questionnaires, while interview protocols followed a structured format to ensure comparability across responses. Triangulation was also applied, using both qualitative and quantitative data to cross-validate findings and improve the robustness of the results.

Results

Demographic Characteristics of Respondents

Understanding the demographic profile of respondents is important for contextualizing their perceptions and experiences regarding physical security management. Regarding to gender distribution, as shown in the table 2, it shows male dominance. Concerning the age distribution, the majority of respondents (72.8%) are within the 18-34 age range, which represents a relatively young university community.

Table 2: Demographic characteristics of respondents

Variable	Categories	Frequency	Percentage
Gender	Female	71	29.7 %
	Male	168	70.3 %
Age	18-24 years	98	41%
	25-34 years	76	31.8 %
	35-44 years	42	17.6 %
	≥45 years	23	9.6 %

Work Experience (Staff)	3-5 years	38	39.2%
	6-10 years	32	33%
	11-15 years	18	18.6
	>15 years	9	9.2 %
Educational Status(staff)	Preparatory	8	8.2%
	Diploma	27	27.8%
	First Degree	30	31%
	Masters	27	27.8%
	PhD	5	5.2%
Educational Status(students)	3rd year	68	47.9%
	4th year	52	36.6%
	5th year ≥	22	15.5%
Respondent Category	Security Personnel	42	17.6%
	Academic Staff	28	11.7%
	Administrative Staff	27	11.3%
	Students	142	59.4%

Source: Field Survey, 2026

Concerning the academic status of respondents, a clear distinction was taken between staff and student respondents. As indicated in the table, only third-year and above undergraduate students were taken. The majority (47.9%) of them were third year students, followed by fourth year students (36.6%) and fifth year and above students (15.5%). This distribution ensures that all student participants have adequate experience to provide informed responses concerning physical security practices and their challenges at the University of Gondar. The majority (72.2%) of staff respondents have between 3-10 years of experience, referring to adequate familiarity with the university's physicals security environment.

Assessment of existing physical security practices

Understanding how security officers protect employees and assets from threats, along with the physical security methods and techniques they employ, is crucial for enhancing physical security at the University of Gondar. Hence respondents were asked to indicate their level of agreement with various statements about existing security practices using a five-point Likert scale (5=Strongly Agree to 1=Strongly Disagree). The results are presented as follow.

Table 3: Respondents' Perceptions of Current Physical Security Practices

No.	Statement	Alternative	Frequency	Percentage
1.	University boundaries (fences, gates) are clearly defined and well-maintained	Agree	31	13 %
		Neutral	19	7.9%
		Disagree	189	79.1%
		Total	239	100%
2.	CCTV cameras are installed in key locations	Agree	28	11.7%
		Neutral	32	13.4%
		Disagree	179	74.9%
		Total	239	100%
3.	Entry to buildings is controlled (guards, Id checks, key cards)	Agree	59	24.7%
		Neutral	17	7.1%
		Disagree	163	68.2%
		Total	239	100%
4.	Outdoor Areas Have Adequate Lighting At Night	Agree	95	39.7%
		Neutral	5	2.1%
		Disagree	139	58.2%
		Total	239	100%
5.	Visible Security Guards Are Regularly Deployed	Agree	165	69%
		Neutral	3	1.3%
		Disagree	71	29.7%
		Total	239	100%
6.	Clear Procedure Exists For Reporting Security Incidents	Agree	82	34.3%
		Neutral	6	2.5%
		Disagree	151	63.2%
		Total	239	100%
7.	Fire Extinguishers And Emergency Exits Are Available And Accessible	Agree	33	13.8%
		Neutral	7	2.9%
		Disagree	199	83.3%
		Total	239	100%
8.	Visitors Are Required To Register At Entry Points	Agree	136	56.9%
		Neutral	5	2.1%
		disagree	98	41%

Source: Field Survey, 2026

The data in table 3 indicates a difference in respondent's perception of current physical security practice at the University of Gondar. Regarding to perimeter security, the data reveals an overwhelming majority (79.1%) disagreed that university boundaries are clearly defined and well-maintained, and only 13% agreed. This refers to serious concerns about the integrity of perimeter fencing and gates, which are fundamental to physical security. In the other hand, concerning CCTV coverage, 74.9% of respondents disagreed that CCTV cameras are installed in key locations, but only 11.7% agreed. This date suggests there is inadequate surveillance coverage across the university campus, which leads to potential blind spots vulnerable to security breaches. Regarding to access control or entry to building, 68.2% disagreed that access is properly managed through security guards and ID checks. Only 24.7 % agreed that access is properly controlled through guards. This reveals weak access control mechanisms what could allow unauthorized individuals to enter building simply. Regarding CCTV, one of key informant interviews from academic staff member commented that:

> *At the University of Gondar, in some areas Cameras are visible, but many Cameras are not functioning. I reported to the concerning body a theft in my office last semester, and when we checked the CCTV, the camera covering that area had been non-functional for months (KII, Academic Staff 2, March 2026).*

Document analysis of security incident reports supported these perceptions, which reveal that that areas with poor lighting and limited CCTV coverage recorded higher incidents of theft and unauthorized access. Concerning the outdoor lighting, a majority (58.2%) disagreed that outdoor areas have adequate lighting at night, while 39.7% agreed that outdoor areas have adequate lighting at night. This data suggests that there is adequate lighting in some areas, but insufficient in other areas, potentially it needs attention night time safety. Regarding to security personnel deployment, majority (69%) of the respondents agreed on the visibility and deployment of security guard and only 29.7% disagreed. This data suggests that human security presence is a relative strength in the current physical security practice at the university.

As shown in table 4.3 above, regarding to incident reporting procedures, 63.2% of the respondents disagreed on the existence of clear procedures for reporting security incidents, but only 34.3% agreed about it. This suggests that there is a poor reporting mechanism to the university community about security incidents. Regarding to fire safety equipment's, majority

(83.3%) of respondents disagreed on the existence and access of fire extinguishers and emergency exits, but only 13.8% agreed. This is the highest negative response in the measurements. This data suggests that there is critical safety vulnerability that requires immediate attention and response. Concerning the visitor's registration process and management system, majority (56.9%) of the respondents agreed that visitors are required to resistor at entry points, but 41% of the respondent disagreed on it. This date indicates that visitor registration procedures exist, but they are not consistently applied across all entry points.

Generally, the above findings propose that even though security guard deployment is perceived positively, most physical security infrastructure elements such as CCTV, boundaries, fire safety equipment, access control, and reporting procedures are perceived as inadequate. This reveals low implementation of physical security practices at the University of Gondar. This finding was also confirmed during key informant interviews, where one security manager stated as flows:

> *At University of Gondar, we have security guards deployed at all entry points and patrols that rotate throughout the campuses. However, the numbers of security guards are insufficient to cover all areas effectively, especially during night shifts (KII, security manager 1, March 2026)*

The key informant interview data provided deeper insights into the current security practices. One of the key informant interviewees (the security chief of the university) described the university's security strategy as follow:

> *To secure the university, our security strategy combines, technology, human resources, and procedures. In our university across campuses, we have approximately 120 security personnel, a CCTV control room with monitoring capacity, and also standard operating procedures, but the security system faces significant challenges such as aging equipment, a limited budget, and the vastness of our campuses make difficult to cover comprehensively (KII, Chief Security Officer; March 2026).*

Concerning the night security system, student council representative express about it as follows:

> *At University of Gondar, we have big security problems. Female students feel unsafe when they walking from the library to dormitories at the night time,*

especially after 9 P.M. there is no adequate light in, and security patrols are infrequent. We have reported this case to the concerning body, but no response and improvements as well (KII, Student Council Representative, March 2026).

According to the revised security policy of the university in 2023, there is a comprehensive provision including incident reporting procedures, access control protocols, and emergency response plans, but the gap between policy and practice was obvious in survey responses and observational data. To protect and make a safe environment of a given organizations, effective physical security practices have a great role. Realizing physical security management is also a crucial for protecting assets, employees, and business operations from a range of pressures. Physical security is not only about protecting physical assets but also it is all about safeguarding employees, ensuring business continuity, and maintaining safe and secure work environment for all (Mishra, 2023). By prioritizing physical security, organizations can deter possible burglars, improve emergency response skills, and maintain stable and secure work environment.

Effectiveness of Existing Physical Security Measures

The study also analyzed the effectiveness of existing physical security measures in safeguarding university assets and personnel. Respondents rated various effectiveness dimensions on a five-point scale and Table 4 presents respondents' perceptions of how effective various physical security measures are in achieving their intended purposes.

Table 4: Perceived Effectiveness of Physical Security Measures

No.	Statement	Alternative	Response	
			Frequenc	Percentag
1.	Access control prevents unauthorized entry	Effective	62	25.9%
		Moderate	8	3.4%
		Ineffective	169	70.7%
2.	Security personnel presence enhances safety perception	Effective	106	44.4%
		Moderate	45	18.8%
		Ineffective	88	36.8 %
3.	CCTV deters crime and vandalism	Effective	38	15.9%
		Moderate	12	5%
		Ineffective	189	79.1%

4.	Security incidents are resolved timely and satisfactorily	Effective	31	13%
		Moderate	8	3.3%
		Ineffective	200	83.7%
5.	Security lighting ensures safe night movement	Effective	57	23.8%
		Moderate	21	8.8%
		ineffective	161	67.4%
6.	Security measures are well-integrated	Effective	62	25.9%
		Moderate	31	13%
		ineffective	146	61.1%
7.	System ensures personal safety of students and staff	Effective	33	13.8%
		Moderate	75	31.4%
		ineffective	131	54.8%
8.	System safeguards university assets	Effective	52	21.8.3%
		Moderate	73	30.5%
		ineffective	114	47.7%

Source: Field Survey, 2026

Regarding the effectiveness of access control, table 4 indicates, a considerable majority (70.7%) rated that access control as ineffective in preventing unauthorized entry, but only 25.9% considering it as an effective. This finding indicates that current access control mechanisms are failing to secure buildings adequately. Concerning to effectiveness of security personnel, it shows that security personnel presence rated the most favorable rating. 44.4% of the respondent considering it as an effective in enhancing safety perception, but 36.8% still rated it ineffective. This finding reveals that even though good presence of security personnel's, still there is room which needs improvement in how security guards perform their duties. The observation check list also revealed that at Maraki Campus, multiple entry points lacked any form of access control, and several CCTV cameras were visibly damaged or improperly positioned. Key informant interview confirms this finding and one of the student respondents provided a specific example as follows:

> *Last month, someone stole my laptop from the library of Maraki Campus. Immediately, I reported it to the concerned body, but the security officer said the CCTV in that section wasn't working. They took my statement but nothing solution*

is given to me. I never got my laptop back (Student Questionnaire, Response 78, March 2026).

Concerning the effectiveness of CCTV deterrence, a considerable 79.1% of the respondents rated CCTV as ineffective in preventing crime and vandalism, and only 15.9% of the respondents considering it effective. This perception suggests that either the cameras are non-functional, poorly positioned, or not perceived as credible threat by potential offenders. Regarding to the effective ness of the incident resolution table 4.4 shows that the most poorly rated measure was incident resolution. Majority (83.7%) of the respondents considers it as an ineffective and only 13% rating it effective. This finding indicates that serious gaps in how security incidents are handled once reported, undermining considerable in the entire security system. The key informant interview confirms the ineffectiveness of conflict it resolution. During interviews, a security supervisor explained that:

When incidents are occurred and reported to us, as much as possible we respond according to procedures, but our capacity is limited due to different factors. We lack vehicles for rapid response, communication tools such as radios are insufficient, and lack of coordination with Gondar city police is sometimes delayed. This affects how quickly and effectively we can resolve incidents (KII, security supervisor, March 2026)

Regarding to the effective ness of security lighting, the night-time safety, 67.4% rated security lighting as ineffective, while only 23.8% considered it effective. This finding verifies the earlier finding about insufficient outdoor lighting and its impact on safe movement at the night time. Concerning to the effectiveness of integration of measures, majority (61.1%) perceived security measures as poorly integrated and only 25.9% considering them well-integrated. This indicates that security components poorly operate rather than as a consistent system. Related to effectiveness personal safety, more than half (54.8%) of the respondents rated the security system as an ineffective in ensuring personal safety of students and staff, while 31.4% of the respondents rated it moderate and only 13.8% of the respondents rated it effective. This finding shows that the university community does not feel sufficiently protected and secured. In the other hand regarding to protection of university assets, 47.7% rated the system as ineffective, 30.5% as moderate, and only 21.8% as effective, which is less negative than some other measures. This finding still represents significant concern for institutional property safeguarding.

The key informant interview finding confirms the ineffectiveness of asset protections. Regarding it, an administrative staff member noted the following idea:

> *Our department has very expensive laboratory equipment, but security is insignificant. Anyone could walk in during working hours without any challenge even though after 5 PM the building is locked, there are no alarm system or motion detectors. It is very vulnerable (KII, Administrative Staff, March 2025).*

To sum up, the finding indicates that security personnel's existence or presence is the only measure with a considerable effective ranking. However, all other measures such as incident resolution, CCTV deterrence, access control, and lighting are supposed as mostly ineffective. This finding indicates that the physical security practice at University of Gondar is ineffective. It also reveals that despite security guards providing some sense of security through presence; it is less effective due to some factors such as lack of modern equipment, inadequate training, and insufficient numbers of security personnel.

Challenge of Physical Security Practices

This study also assessed the main challenges of physical security practice at the university. Respondents rated various potential challenges.

Table 5: Challenges Affecting Physical Security Management

No.	Statement	Alternative	Response	
			Frequency	**Percenta**
1.	Insufficient funding for security equipment, maintenance, and personnel	Challenge	169	70.7%
		Moderate	60	25.1%
		Not Challenge	10	4.2%
2.	CCTV, alarms, or access systems are old, broken, or poorly maintained	Challenge	158	66.1%
		Moderate	60	25.1%
		Not Challenge	21	8.8%
3.	Not enough guards, leading to poor coverage or long shifts	Challenge	128	53.6%
		Moderate	75	31.4%
		Not Challenge	36	15%
4.	Security systems haven't kept pace with growth in buildings and student numbers	Challenge	172	71.9%
		Moderate	61	25.5%
		Not Challenge	6	2.5%
5.	Security staff not adequately trained in	Challenge	160	67%

	modern techniques	Moderate	51	21.3%
		Not Challenge	28	11.7%
6.	Community not security-conscious, ignore protocols, fail to report	Challenge	66	27.6%
		Moderate	110	46%
		Not Challenge	63	26.4%
7.	Poor communication between security, administration, and police	Challenge	127	53.1%
		Moderate	82	34.3%
		Not Challenge	30	12.6%
8.	Poorly designed buildings that aid criminals (CPTED issues)	Challenge	132	55.2%
		Moderate	65	27.2%
		Not Challenge	42	17.6%

Source: Field Survey, 2026

Table 5 represents respondents' perception of various challenges that affect physical security practices at the University of Gondar. The results of this study indicated that the challenges of physical security practice at University of Gondar were categorized as resource-related challenges, personnel-related challenges, coordination and design-related challenges, policy-related challenges, and community-related challenges.

Resource and Financial Related Challenges

The survey finding shows that the most critical challenge identified was that security systems haven't kept pace with growth. 71.9% of the respondents rated it as a challenge, and only 2.5% of the respondents disagreed. This finding reveals that the reality of rapid university expansion without corresponding security infrastructure development. The key informant interview confirms that there is rapid expansion of university infrastructure without corresponding security upgrades. A facility manager noted that:

> *In our university when new buildings are constructed, security is often not considered. For example, during design of the construction main elements such CCTV camera, access control points and security rooms should incorporate, but in practice most of the time they aren't considered (KII, Facilities Manager; March 2026).*

Regarding funding for physical security practice, the majority (70.7%) of the respondents perceived that insufficient funding as a challenge, but only 4.2% of the respondent disagreed about it. The third data indicate that limited funds are primary hindrances for effective security

management at the university. This financial limitation can affect technological material maintenance, acquisition of equipment (like CCTVE camera and communication radios) and security personnel. Some of the key informant interview also confirms that financial limitations are the most serious challenge in our institution. One of the chief security officers explained that:

> *Budgetary constraints are the major problem in our university. The annual budget for security has remained stagnant, while the University expands overtime. The student enrolment increases from time to time, but the budget remains constant and it does not reflect the realities. We have limited vehicles, we need new CCTVE Cameras, more personnel, and modern access, but we can only afford minimal upgrades each year (KII, Chief Security Officer; March 2026).*

Finding obtained from document analysis confirms the above survey data. According to 2024/2025 fiscal year annual budget, the security sector receives approximately 3.2% of the non-academic operational budget, which is inadequate given the university's size and risk profile. For example, one of security supervisor explained about the constraints of the budget:

> *Across all campuses, we have only 3 patrol vehicles, but only 2 of them are operational. We have limited funds for timely repairs. Concerning to communication radios, we have only 5 and 3 of them are working properly; even it is not enough for effective coordination. These gaps directly and indirectly affect our response capability for security system (KII, Security Supervisor; March 2026).*

Concerning broken and outdated equipment's, 66.1% of the respondents identified it as challenge, and this finding reveals that while security technology exists; it is often out dated. Observation check list also confirmed this finding. As the researchers observed, maintenance issues and technological uselessness are very challenge for security system at the university. The researchers observed that at the main campus out of 20 CCTV cameras, 12 of them are non-functional. At Maraki Campus, out 15, 8 cameras were clearly damaged. Regarding to alarm security system, none of the observed buildings have visible none of the observed buildings had visible interruption detection security systems. The key informant interview data also confirmed this finding. One of the security control room operators explained that:

> *In our campus, we have only 8 screens in monitoring center. However, most of them show static or blank feeds since cameras are broken. We always report about the*

faulty cameras, but no one gives you response. It takes months for repair (KII, Security Control Room Operator; March 2026).

Human Resource Related Challenges

Regarding insufficient training, 67% of the respondents perceive it as a challenge, but only 11.7% of the respondents disagreed about the inadequacy of training. This data reveals that the security personnel have lack of knowledge and skill to address the modern security threats effectively. 53.6% of the respondents also identified as a challenge the insufficient guards. This finding shows limited security guards leads to difficult to cover and potentially exhausted personnel working for long shifts. The key informant interview finding confirms about the inadequacy of staffing and training gaps. For example, one of the security guards shared that:

We have limitation of human power, due to this reason; we work for 12-hour in one day. During night shifts, one patrol alone covers a large area. It is exhausting and dangerous. If something happens, it is difficult to respond quickly (KII, Security Guard; March 2026).

Concerning security guards training, a security trainer explained that:

New recruits get only two weeks of basic training which covering security issue, patrolling, report writing, and basic first aid. But there is no continuous professional development to improve security guards knowledge. We haven't taken training on modern security technology and cyber-physical security integration. When new systems are installed, we learn through experience, which isn't effective (KII, Security Training Officer; March 2026).

Coordination and Design Related Challenges

The survey data shows, majority (53.1%) of the respondents perceived that there is poor communication between security, police and administration regarding to security concern regularly. This data indicates that the availability of coordination gaps among stakeholder concerning the securities that undermine integrated security responses. The building design issues were also rated as a challenge by majority (55.2%) of the respondents. This shows physical infrastructure itself facilitates rather than prevents security breaches. Key informant interviews replied that coordination with Gondar city police occurs rarely for major incidents. A security manager replied:

We have rarely meetings with Gondar city police to discuss about security issue, but during emergencies, response times are unpredictable. There is no regular and formal communication of understanding defining roles, response protocols or responsibilities. This uncertainty affects our security management capability coordination (KII, Security Manager; March 2026).

Community Related Challenges

The data in the table above shows that community security awareness rated as the most balanced distribution measurement. 46% of the respondents perceive it as moderate, 27.6% of the respondent rated it as challenge, and 26.4% of the respondent rated it as not a challenge. This data reveals despite community awareness is not the most concerning security issue, it remains a moderate security concern requiring attention. In this regard, many respondents responded that students and staff contribute to security vulnerabilities. One of the students wrote; "*most of the students usually support open secure doors for suitability, we share ID cards, and we do not care about the security instructions. We are not conscious security threats until something happens" (Student Questionnaire, Response 112; March 2026).*

One of the members of academic staff explained that "faculty members are often remains silent when they see unfamiliar people in hallways. We assume that everyone members of the university. This openness, even though it philosophically aligned with academic freedom, creates security gaps (KII, Academic Staff; March 2026)".

Vulnerable Locations

Respondents were asked to identify particularly vulnerable or unsafe locations at the study areas and thematic analysis of the respondents revealed the following finding (Table 6).

Table 6: Frequently Identified Vulnerable Locations

Location	**Frequency Mentioned**	**Primary Concerns**
Library back entrance	42	Poor lighting, no CCTV, unauthorized access
Maraki Campus parking area	38	Theft from vehicles, poor lighting
Student dormitory pathways	35	Night safety concerns, insufficient patrols
Science laboratory complex	31	Valuable equipment, limited access control

Main Campus back gate	29	Unauthorized entry, infrequent checks
Fasil Campus peripheral areas	24	Boundary breaches, isolated location

Source: Field Survey, 2026

Generally, the findings reveal that resource limitations particularly failure to keep pace with growth, inadequate funding, out-dated equipment, and insufficient training are the most critical challenges facing physical security management at the University of Gondar. To ensure validity and reliability of the data, finding from different data source were triangulated and table 7 summarizes the triangulation across methods as follow.

Table 7: Triangulation of Data

Theme	**Survey finding**	**Interview finding**	**Observation findings**	**Conclusion**
Perimeter security	79.1% disagree boundaries are well	Identified as top vulnerability	Multiple gaps observed	It is confirmed that the perimeter
CCTV Coverage	74.9% disagree cameras in key locations	Described as non-functional	Cameras appear non functional	It is confirmed that the CCTV system is ineffective
Access Control	68.2% disagree entry is controlled	Identified as critical vulnerability	Unlocked windows observed	It is confirmed that the access control is weak
Security Personnel	69% agreed that guards are visible	Acknowledged as relative strength	Guards visible but alertness varies	It is confirmed that the human presence is a strength but quality issues exist
Fire Safety	83.3% disagree equipment available	Not specifically mentioned	Missing extinguishers, faded signs	It is confirmed that critical fire safety gap

Discussion of the study finding

Regarding to the current physical security practice at the University of Gondar, the finding reveals that the security guard deployment is the only relatively strong practice. However, CCTV coverage, access control, perimeter security, and fire safety equipment are perceived as inadequate. In the other hand, visitor registration and outdoor lighting show mixed results. Related to the effectiveness of security measures taken at the university, the finding suggests that the overall effectiveness is low across most measures. Measures like incident resolution, access control, and CCTV deterrence are rated the most ineffective. Relatively, security personnel presence receives the highest effective measures. This finding presents both support and challenges for existing literature. In the case of supportive, the finding that the security personnel deployment is the most visible physical security practice and aligns with Filippov (2019), who suggest that in many developing country contexts, security personnel remain the backbone of physical security due to lower implementation cots compared to technological solution. In addition, higher education institution s resources-constrained environments often prioritize human security presence over technological infrastructure. The insufficient perimeter security finding supports (Karlos and Larcher, 2020), who emphasized that inadequately maintained boundaries create fundamental vulnerabilities in any security system.

Concerning to the challenges affecting physical security at the University of Gondar, the finding reveals that resource limitations such as funding, staffing and equipment are the most critical challenges. Furthermore, the findings suggest that the security systems haven't kept pace with institutional growth. Inadequate training, poor coordination multifaceted challenges and building design and policy communication are moderate concerns. Generally, the triangulation of the finding confirms consistency across data sources, strengthening validity of the findings. The convergence of evidence from multiple methods suggests that the identified practices, effectiveness level, and challenges correctly reflect the reality of physical security management practice at the University of Gondar. It reveals that physical security practices at the University Gondar faces systematic challenges which requiring comprehensive intervention. Related to the theoretical alignment, the finding confirms that the applicability of routine activity theory (like convergence of offenders, targets and absent guardianship), crime prevention through

environmental design (environmental design deficiencies) and system theory (interdependence failures) can explain the current physicals security situation at the University of Gondar.

The sheer findings pertaining to security practices at the University of Gondar is consistent with Asangausung et al.(2024), observations who suggest that perimeter security is usually neglected in higher education institutions due to budget constraints and the perception that fences are less critical than active security measures. From the finding, 83.3% of the respondents disagreed on the existence of fire extinguishers and emergency exits and it represents a major safety gap. This finding is consistent with Ategwu (2025) idea. Fire safety is frequently overlooked in higher education institutions almost in all Sub-Saharan Africa. However, this finding contradicts the international standards recommended by the International Fire Safety Standards (Gao et al., 2026), which suggest that all educational institutional maintain accessible fire safety materials and conduct regular trainings. On the other hand, the findings that 74.9 % of the respondents disagreed on the idea that CCTV camera are installed in key locations. This finding challenges the assertion by Pacapac (2022) which suggest that higher education institutions in developing countries are increasingly adopting surveillance technologies. The observation finding that out of 20 CCTV cameras on the main campus, 12 were nonfunctional; suggest that even where technologies were exists, maintenance failures render it ineffective.

When we see the theoretical integration, applying routing activity theory, the inadequate physical security practices creates conducive environment to crime. The lack of functional CCTV, poorly maintained boundaries, and weak access control to together explain the incidents reported at University of Gondar. When any of the three elements such as motivated offender, absences of guardians, and suitable target coverage, crime become likely (Ahmad and Ramayah, 2022). From the perspective of CPTED, the University of Gondar demonstrates critical limitations in all four-crime prevention through environmental design principles. Asundi (2022) also argued that environment that fail to implement crime prevention through environmental design principles actively facilitate criminal activities than preventing it.

Conclusions and Study Implication

Conclusion

The study grounded in three basic theoretical frameworks: crime prevention through environmental design, routine activities theory and systems theory. Both quantitative and

qualitative results of the study indicated that security officers' overall practices of physical security management are insufficient. Most of the security officers consider University of Gondar did not give adequate prioritization for physical security. There are gaps that the University should consider to give prioritization of physical security management. The result also shows that there are insufficient security measures to prevent crime and ensure safety. Even though insufficient, the finding shows security personnel deployment was the most visible practice, with guards present at major entry points and conducting patrols. In the other hand visitor registration and access control were moderately implemented but inconsistently enforced, with side entrances often uncontrolled. CCTV coverage, outdoor lighting, and fire safety equipment were the least adequate practices, with many cameras non-functional, poorly lit areas, and inaccessible or missing fire safety equipment. This can affect the effectiveness access control and creates potential vulnerability. These are the major problem to physical security management in the university which may lead to undermine the deterrent effect of surveillance and immediate respond to security incidents.

All security measures were perceived as low across most measures. The finding reveals that the security personnel presence was rated relatively effective; which provides some sense of safety despite limitations. The finding also shows that access control system, incident resolution process, CCTV deterrence and assets protection system were perceived as the most ineffective.

Finally the finding identifies insufficient funding (such as stagnant budgets, limited equipment, maintenance, and personnel), Out-dated technology (such as non-functional CCTV, no intrusion detection, and lack of repairs), inadequate staffing, failure to keep pace with expansion (like new buildings without corresponding security upgrades), inadequate training (minimal initial training, no continuous professional development), low community awareness, poor coordination, policy gaps, and CPTED deficiencies (poorly designed buildings aiding criminal activity) were the main challenges. Students' dormitory pathways, science laboratory complexes, Maraki Campus parking area and library back entrance were also identified as specific vulnerable locations.

Implications of the findings

To solve the challenges and improve the effectiveness of physical security practice at the University and to create conducive environment for the community the University administration and leadership should conduct all-inclusive security audit and master planning; dedicates

security budgets to upgrade infrastructure, to maintain security equipment's, and to increase security personnel; provide comprehensive training program and the training should be continuous professional development and improve working conditions. The security department should integrate technology in the security system and maintain the broken technologies; standardize and enforce security procedures, implement and enforce access control policy across all entry points such as mandatory ID checks for all staff, students, and visitors; and consider the crime prevention through environmental design principles when they design building and expand campuses. The University Security Management Division should launch security awareness and engagement campaign. The University Community should also create standing security committee which contains representatives from administrations, students, security personnel, and faculty.

Data Availability Statement

The authors confirm that the data gathered are included in this manuscript, and any additional data supporting the findings of this study are available from the corresponding author upon request.

Acknowledgments

We would like to thank all the participant of the study. Our appreciation also goes to individuals and stakeholders participated in the study process.

Disclosure

There is no conflict of interest in this study.

Reference

Ahmad, I., Aisha, A., Kabir, A., & Abdullahi. (2023). Relevance of system theory to open and close systems in organisational management. *Journal of Management and Social Sciences*, 7, 145-158.

Ahmad, R., & Ramayah, T. (2022). A systematic literature review of routine activity theory's applicability in cybercrimes. *Journal of Cyber Security and Mobility*, 11(3), 333-366. https://doi.org/10.13052/jcsm2245-1439.1133

Alemie, A., & Belaye, H. M. (2018). Nature, benefits, challenges and opportunities of university-community engagement: In the case of University of Gondar, Ethiopia. International

*Journal of Research on Service-Learning and Community Engage*ment, 6(1), 1-18. https://doi.org/10.37333/001c.7022

Alexei, A. (2021). Network security threats to higher education institutions. In Central and Eastern European eDem and eGov Days (Vol. 341, pp. 241-252). Verlag der Technischen Universität Graz. https://doi.org/10.24989/ocg.v341.24

Asangausung, O., Abang, T., Oko, N., Okon, G., & Wealth, J. (2024). An assessment of the challenges of public and private security organisations in Nigeria. *AKSU Journal of Social Sciences*, 4(2), 134-146.

Asundi, S. (2022). Crime prevention through environmental design (CPTED) best practices. *International Journal of Intelligent Systems and Applications in Engineering*, 10(2), 322-325.

Ategwu, P. 2025. Management of safety and security in education for sustainable national development. *Journal of Educational Studies*, 12(1), 45-62.

Aven. (2015). Risk Analysis. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

Bács, Z. (2022). National security and higher education: Challenges, risks and threats. *Nemzetbiztonsági Szemle*, 10(3), 91-99. https://doi.org/10.32561/nsz.2022.3.9

Boateng, F. (2020). Higher education systems and institutions, Ethiopia. *In The international encyclopedia of higher education systems* (pp. 1-12). Springer. https://doi.org/10.1007/978-94-017-9553-1_449-1

Clancey, G., & Fisher, D. (2016). Crime prevention through environmental design in New South Wales. *Australian Planner*, *53*(2), 73–82. https://doi.org/10.1080/07293682.2015.1118392

Coole, M. P., & Brooks, D. J. (2021). Physical Security: Best Practices. In *Encyclopedia of Security and Emergency Management* (pp. 730–737). Springer, Cham. https://doi.org/10.1007/978-3-319-70488-3_220

Dar, W. (2022). Security framework: A case study of a higher education institution. *International Journal of Security and Privacy*, 4(2), 45-58.

DiMaggio, P.J. and Powell, W.W. (1983) The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. American Sociological Review, 48, 147-160. https://doi.org/10.2307/2095101

Ekpoh, U., Edet, A., & Ukpong, N. (2020). Security challenges in universities: Implications for safe school environment. *Journal of Educational and Social Research*, 10(6), 112-123. https://doi.org/10.36941/jesr-2020-0113

Fennelly, L. (2016). Effective physical security (5th ed.). *Butterworth-Heinemann.*

Filippov, D. (2019). Components of physical security risk. Issues of Risk Analysis, 16(4), 82-93. https://doi.org/10.32686/1812-5220-2019-16-4-82-93

Gao, Z., Yu, G., Yu, Z., & Xing, K. (2026). Hazard-source-based review of fire safety in building-integrated photovoltaics. *Solar Energy*, *316*, 114837. https://doi.org/10.1016/j.solener.2026.114837

Hadidane, S., & Khelalfa, H. (2023). The role of the university in modern society. *Journal of Higher Education Studies, 7(1), 8-22.*

Harney, B. (2024). Systems theory. In Elgar encyclopedia of business management (pp. 321-334). *Edward Elgar Publishing*. https://doi.org/10.4337/9781035308767.ch41

Jonek-Kowalska, I. (2022). Determinants of Risk Management Effectiveness: Previous Research and Conclusions. In I. Jonek-Kowalska (Ed.), *Effectiveness of Enterprise Risk Management: Determinants and Opportunities for Improvement* (pp. 1–21). Springer International Publishing. https://doi.org/10.1007/978-3-030-95376-8_1

Karataş, A. (2021). Evaluation of security management from the perspective of current management approaches and management models. *Journal of Academic Social Resources*, 6(28), 1653-1670. https://doi.org/10.31569/ASRJOURNAL.369

Karlos, V., & Larcher, M. 2020. Guideline: Building perimeter protection - Design recommendations for enhanced security against terrorist attacks. *Publications Office of the European Union*. https://doi.org/10.2760/20368

Landucci, G., Khakzad, N., & Reniers, G. (2020). An introduction to physical security. In Security and risk assessment for chemical facilities (pp. 1-25). *Elsevier*. https://doi.org/10.1016/B978-0-444-64054-3.00001-9

Masum, M. R., & Training, T. (2024). Introduction to physical security and physical security measures training. *Security Management Review*, 11(4), 33-48.

Mishra, A. (2023). Effective Physical Security Protocols 2023. *Corp Security Team*. https://corpsecurity.org/effective-physical-security/

Mishra, P., & Paney, K. (2024). Challenges for higher education and their solutions. ShodhKosh: *Journal of Visual and Performing Arts*, 5(1), 1 15. https://doi.org/10.29121/shodhkosh.v5.i1.2024.5674

Nuamah Eshun, S., & Salifu, I. (2025). Challenges of campus security guards in Ghanaian higher education: A case of a university's satellite learning centers. *Journal of Higher Education Policy and Managemen*t, 47(2), 189-205. https://doi.org/10.1080/1360080X.2025.2469941

Onuorah, H., Eziamaka, C., & Nonye. (2020). Assessment of physical security management practices applied by principals for ensuring safety in secondary schools in Anambra State. *Journal of Educational Leadership*, 5(3), 2251-0303.

Pacapac, M. T. (2022). Security practices of higher education institutions in Ilocos Norte, Philippines in the upsurge of coronavirus. *Jurnal Pendidikan Progresif*, 12(3), 1473-1491. https://doi.org/10.23960/jpp.v12.i3.202235

Reason, J. (1990). Human Error. Cambridge University Press, Cambridge. https://doi.org/10.1017/CBO9781139062367

Riskhan, B. (2024). Physical security to cyber security: Challenges and implications in the modern digital landscape. *Journal of Electrical Systems*, 20(4), 692-702. https://doi.org/10.52783/jes.2090

Sasse, S. (2005). "Motivation" and Routine Activities Theory. *Deviant Behavior*, *26*(6), 547–570. https://doi.org/10.1080/01639620500218260

Steinmetz, K. F. (2025). Routine Activities Theory? A Kindly Critique and a Pathway Forward. *Victims & Offenders*, *20*(5–6), 798–813. https://doi.org/10.1080/15564886.2025.2476681

Taherdoost, H. (2022). *What are Different Research Approaches? Comprehensive Review of Qualitative, Quantitative, and Mixed Method Research, Their Applications, Types, and Limitations* (SSRN Scholarly Paper No. 4178694). Social Science Research Network. https://papers.ssrn.com/abstract=4178694

Wen, Y., Qi, H., Long, T., & Zhang, X. (2025). Designed for safety: Characteristics and trends in crime prevention through environmental design research. *Journal of Asian Architecture and Building Engineering*, *24*(4), 3108–3126. https://doi.org/10.1080/13467581.2024.2366823