International Journal of Safety and Security Engineering
Vol. 15, No. 10, October, 2025, pp. 2121-2134
Journal homepage: http://iieta.org/journals/ijsse

Enhancing Security Service Efficiency Through Risk Management: Analyzing the Impact of Employee Leave Patterns at King Saud bin Abdulaziz University for Health Sciences

Khaled Mili*, Shaykhah Abdullah Aldossari

Department of Quantitative Methods, College of Business, King Faisal University, Al-Ahsa 36362, Saudi Arabia

Corresponding Author Email: kmili@kfu.edu.sa

https://doi.org/10.18280/ijsse.151015

Received: 11 September 2025
Revised: 12 October 2025
Accepted: 23 October 2025
Available online: 31 October 2025

Keywords:
risk management, security services, higher education, employee leave, patterns, workforce management, Monte Carlo simulation

ABSTRACT

Security service efficiency in higher education institutions depends critically on workforce availability, yet the relationship between employee leave patterns and operational performance remains understudied. This study investigates this relationship at King Saud bin Abdulaziz University for Health Sciences through mixed-methods research combining quantitative analysis of 2,363 leave instances (2022-2024), surveys of 160 stakeholders, and semi-structured interviews with 15 security managers. Temporal analysis identified pronounced leave clustering on weekends (45.9%) and during January, August, and November. Correlation analysis revealed significant relationships between absence rates and security coverage ($r = -0.71$, $p < 0.001$), incident response times ($r = 0.74$, $p < 0.001$), and incident frequency ($r = 0.68$, $p < 0.01$). Monte Carlo simulations of three risk mitigation scenarios demonstrated that comprehensive leave management could reduce response times by 37.4% and incidents by 48.6%, with projected annual net benefits of SAR 330,000. Findings establish absence management as a critical component of security risk management in educational institutions.

1. INTRODUCTION

Universities represent complex ecosystems where diverse populations converge, valuable assets are housed, and sensitive information is managed, creating multifaceted security challenges that require sophisticated approaches to risk management. Wang and Hu [1] demonstrated that effective campus risk assessment must employ quantitative methods that account for risk interactions rather than treating threats as isolated factors. The effective delivery of security services within these environments has direct implications for institutional reputation, operational continuity, and the well-being of students, faculty, and staff.

In recent years, educational institutions worldwide have witnessed an evolution in security threats, ranging from unauthorized access to critical facilities to cybersecurity breaches. Effective security management requires integrated approaches; Soomro et al. [2] demonstrated this principle in information security contexts, arguing that technical systems, organizational policies, and human factors must be addressed holistically rather than in isolation. This changing landscape has necessitated a shift from reactive security measures to proactive risk management approaches. Aleem et al. [3] emphasized the importance of converged security approaches that integrate physical and information security systems, addressing vulnerabilities that emerge when these domains operate in isolation. Despite these advances, a critical yet often overlooked factor affecting security service performance is the management of human resources, particularly employee leave patterns and their impact on operational continuity.

The relationship between workforce availability and security effectiveness represents a significant challenge for security management. Johns [4] noted that attendance dynamics in the workplace directly affect service quality and operational efficiency, especially in sectors requiring continuous presence, such as security services. When security personnel are absent, coverage gaps may emerge, potentially compromising the institution's security posture and increasing vulnerability to various threats. This relationship between personnel availability and security effectiveness has received limited attention in the scholarly literature, particularly in the context of higher education institutions.

King Saud bin Abdulaziz University for Health Sciences, as a leading educational institution in Saudi Arabia, presents an ideal setting for investigating these dynamics. The university's commitment to providing a safe educational environment for its community members, coupled with the sensitive nature of its health-focused academic programs and facilities, creates a compelling case for examining how risk management practices, particularly those addressing workforce availability, influence security service outcomes.

Preliminary observations at the university indicate significant variations in employee leave patterns throughout the week and year, with potential implications for security coverage and incident response capabilities. These patterns raise important questions about how security services can be optimized to maintain effectiveness despite fluctuations in workforce availability. While existing literature has addressed security management challenges in organizational contexts, from information security implementation [5] to campus safety operations [6], there remains a gap in understanding how employee leave patterns specifically affect physical security service performance and how risk management strategies can address these challenges.

This study aims to investigate the relationship between risk management strategies and security service efficiency at King Saud bin Abdulaziz University for Health Sciences, with particular emphasis on the impact of employee leave patterns. Specifically, the research seeks to:

1. Analyze patterns in security personnel leaves over a three-year period (2022-2024) and identify temporal trends and correlations
2. Evaluate the relationship between leave patterns and key security performance indicators, including incident response time and frequency of security incidents
3. Develop and assess potential scenarios for improving security service efficiency through enhanced leave management and risk mitigation strategies
4. Propose evidence-based recommendations for optimizing security operations in university settings

The significance of this research extends beyond its immediate context. Educational institutions globally face similar challenges in managing security services with limited resources. By providing empirical evidence on the relationship between leave patterns and security outcomes, this study contributes to a deeper understanding of operational challenges in university security services. Furthermore, the methodological approach incorporating Monte Carlo simulations offers a framework for predictive analysis that can be adapted to diverse institutional contexts.

The subsequent sections of this paper present a review of relevant literature, outline the methodology employed, report and discuss the findings, and offer conclusions and recommendations for practice and future research. Through this structured approach, the study aims to enhance understanding of how risk management practices can improve security service efficiency in higher education settings, particularly through effective management of workforce availability.

2. LITERATURE REVIEW

This section examines the existing body of knowledge related to security risk management in educational institutions, with particular focus on workforce management challenges and their impact on security service effectiveness. The review is organized thematically to establish the theoretical foundations for the current study and identify gaps in the literature that this research addresses.

2.1 Risk management in educational institutions

The concept of risk management in educational settings has evolved significantly over the past decades. Masmali and Miah [7] conducted a comprehensive analysis of risk management practices in Saudi public sector organizations, highlighting that educational institutions face unique challenges due to their open environments, diverse populations, and complex operational requirements. Similarly, Ulven and Wangen [8] identified security management challenges in educational institutions globally, emphasizing the need for integrated approaches that balance security imperatives with academic freedom.

The application of formal risk management frameworks in university settings has gained increased attention following high-profile security incidents at educational institutions worldwide. The evolution of campus security following high-profile incidents has led to more structured security approaches. Contemporary research [9] demonstrates that these practices, including situational crime prevention techniques and visible security presence, are positively associated with students' perceptions of safety, providing empirical validation of modern security frameworks. However, as Fox and Savage [10] noted, many institutions still struggle with translating risk management theory into practical security measures that address the specific needs of academic environments.

Yang [11] proposed a comprehensive campus security management framework adapted for the Internet age, emphasizing technology integration, intelligent monitoring systems, and data-driven security operations. While such frameworks advance technological capabilities, they typically do not specifically address the human resource dimensions of security operations, particularly workforce availability patterns.

Recent research in IJSSE has advanced the understanding of risk management implementation in institutional contexts. Petryshyn et al. [12] developed a comprehensive risk management system for engineering enterprises, emphasizing the integration of security considerations with operational efficiency, an approach parallel to this study's focus on workforce-security relationships. Similarly, Berrada et al. [13] demonstrated that technology-enabled risk management systems improve both monitoring capabilities and response effectiveness, findings that inform the technology integration components of our improvement scenarios (Section 4.4).

2.2 Security service management in higher education

Managing security services in higher education poses distinct challenges compared to other sectors. A study by the University of Alberta identified inadequate resources, convoluted operational procedures, and a lack of specialized training for security professionals as major obstacles confronting university security departments. The Business Officers Association further noted that balancing security needs with the open nature of academic environments necessitates specialized approaches, differing from those utilized in corporate or government settings.

Alshareef [14] developed an information security risk management framework for Saudi Arabian government organizations, revealing significant variation in implementation levels across institutions. While focused on cybersecurity, the study's findings about implementation gaps, including the need for comprehensive planning and staff training, parallel challenges in physical security service delivery.

Research on security service delivery underscored the critical role of human capital, highlighting the importance of specialized training for security personnel in educational settings. However, studies examining how workforce availability affects security outcomes remained limited. The study argued that the unique nature of campus environments requires security staff to develop skills beyond those typically associated with security work in other contexts but did not examine how workforce availability affects security outcomes. Effective security service management requires integrated approaches that address multiple dimensions simultaneously. Soomro et al. [2] argue that security management, whether addressing physical or information security, needs holistic frameworks integrating technical systems, organizational policies, and human factors rather than treating these as isolated components. This principle extends to workforce management, where absence patterns, technological capabilities, and operational procedures must be coordinated systematically.

2.3 Workforce management in security services: Sector-specific characteristics

While workforce absenteeism affects organizational performance across sectors, security services in educational institutions present distinct operational characteristics that differentiate them from typical university staff roles. Understanding these distinctions is essential for contextualizing this study's focus on security-specific absence patterns.

2.3.1 Continuous operation requirements

Security services demand 24/7 operational continuity regardless of weekends, holidays, or organizational schedules. This distinguishes security from administrative, academic, and most support functions that operate during standard business hours. Johns [4] demonstrated that attendance dynamics vary substantially between continuous-operation and standard-hour environments, with continuous operations showing higher baseline absence rates and greater operational impact per absence event.

Comparative research in emergency services reveals similar patterns. Shift-based protective services (police, fire, emergency medical) exhibit absence clustering around weekends and holidays that create disproportionate coverage challenges compared to day-shift administrative roles [15]. When administrative staff are absent, tasks may be delayed or redistributed; when security personnel are absent during critical coverage periods, organizational vulnerability increases immediately.

This temporal inflexibility creates unique planning challenges. Universities operate continuously despite varying activity levels—weekends see reduced academic activity, but facilities remain occupied, creating security demands that persist independent of the institutional calendar. Consequently, security workforce management requires fundamentally different approaches than academic or administrative human resource planning.

2.3.2 Non-substitutability of security functions

Security personnel possess specialized training, certifications, and authorized response capabilities that prevent casual task redistribution during absences. This parallels healthcare settings where adequate staffing levels are essential: research demonstrates that clinician staffing directly affects service delivery costs and outcomes [16], as specialized healthcare functions cannot be maintained through simple workload redistribution. However, security faces an additional constraint: deterrence value depends on visible authorized presence, not merely task completion.

In administrative contexts, employee absence may reduce throughput or delay projects, but work often accumulates for later completion or is redistributed among colleagues. Security coverage gaps cannot accumulate—each hour of inadequate coverage represents irreversible risk exposure. This non-substitutability distinguishes security from fungible organizational functions, where cross-training enables flexible staffing.

Our study addresses this gap by measuring performance degradation across varying absence levels, demonstrating that security effectiveness cannot be maintained through simple workload redistribution strategies effective in other university departments.

2.3.3 Visible presence and deterrence theory

Security services derive effectiveness partly from preventive deterrence—the visible presence that influences potential offenders' risk calculations [17]. This mechanism operates independently of active interventions, distinguishing security from reactive service functions. Administrative absences affect output; security absences reduce deterrent presence, potentially increasing incident probability.

Deterrence theory in criminology establishes that perceived surveillance and sanctions certainly influence behavior [18]. Applied to campus security, this implies that reduced visible presence during high-absence periods may alter risk perceptions among community members, potentially increasing opportunistic violations. While comprehensive deterrence research in university settings remains limited, the theoretical foundation suggests security workforce availability affects outcomes through mechanisms absent in non-protective services.

Campus security effectiveness depends on both response capability and visible presence, with presence serving preventive rather than reactive functions. This dual-purpose nature, preventing incidents through presence while responding to those that occur, creates staffing requirements distinct from single-function roles.

2.3.4 Comparative absence patterns across sectors

Limited comparative research examines absence patterns across occupational sectors within universities. General organizational research establishes baseline absence rates of 8-12% in professional office environments [4], compared to 15-18% in continuous-operation protective services. However, few studies isolate security specifically or examine how absence impacts operational outcomes differently across sectors.

Aldoghan and Elrayah [19] examined absenteeism policies across Saudi organizations without sector-specific analysis, while Maroney [20] documented absenteeism's organizational costs generally without distinguishing operational contexts. This gap justifies a focused examination of security sector dynamics rather than extrapolating from general workforce research.

The Role of Absenteeism Within Female Staff explored gender-specific patterns but did not address occupational differences in absence consequences. Research in healthcare settings demonstrates parallel staffing challenges: Han et al. [16] found that adequate clinician staffing levels significantly affected service delivery costs and quality in community health centers, illustrating how workforce availability directly impacts operational outcomes in service-intensive environments—a dynamic analogous to security services. Our study contributes by establishing that security services require a specialized workforce analysis distinct from general human resource management frameworks.

2.3.5 Theoretical framework: Security as continuous protective service

Synthesizing these characteristics, security services in educational settings constitute a distinct occupational category: continuous protective services. This classification shares more characteristics with emergency services (police, fire, emergency medical) than with typical university staff roles:

1. **Temporal structure:** 24/7 continuous operation vs. scheduled business hours
2. **Functional substitutability:** Low substitutability due to specialized authorization vs. high substitutability in administrative roles
3. **Output accumulation:** Non-accumulable (coverage gaps cannot be "made up") vs. accumulable (delayed work can be completed later)
4. **Effectiveness mechanisms:** Preventive presence plus reactive response vs. primarily reactive task completion

This framework establishes why security workforce management demands specialized approaches. General human resource practices developed for standard administrative contexts may prove inadequate when applied to continuous protective services without adaptation for these distinguishing operational characteristics.

Existing literature addresses various aspects of security management in educational settings [5, 6], and workforce absenteeism broadly [21, 22], but a systematic examination of how these factors interact specifically in security contexts remains limited. This study addresses that gap by quantifying relationships between workforce availability and security outcomes in a continuous protective service environment.

2.4 The use of simulation techniques in security management

Simulation modeling has emerged as a valuable tool for analyzing complex security management issues and evaluating the effectiveness of risk mitigation strategies. In the context of higher education, researchers have increasingly employed Monte Carlo simulations to explore the impact of various factors on security operations, including resource allocation, staffing levels, and incident response capabilities [7].

For example, a Monte Carlo simulation study was conducted to examine the optimal allocation of security resources at a university campus, considering the spatial distribution of potential threats and the mobility of security personnel. utilized similar simulation techniques to assess the effectiveness of different security surveillance strategies in a university setting, incorporating factors such as camera coverage, response times, and the probability of threat detection.

While these studies have provided valuable insights into the application of simulation techniques in university security management, they have primarily focused on the logistical and operational aspects of security service delivery. The present study aims to expand on this research by incorporating the human resource dimension, specifically the impact of employee leave patterns, into the security management simulation framework.

3. METHODOLOGY

3.1 Research design

This study employed a mixed-methods design combining quantitative analysis, qualitative inquiry, and simulation modeling to examine relationships between employee leave patterns and security service efficiency. The approach integrates descriptive analytics of historical data with stakeholder perspectives and predictive scenario analysis, enabling triangulation across multiple evidence sources.

The research utilized a single-case study design [23] focused on King Saud bin Abdulaziz University for Health Sciences. While single institution designs limit generalizability, they enable deep contextual understanding and access to comprehensive operational data unavailable in multi-site studies. The institution's characteristics—health sciences focus, public university status, and Saudi Arabian context—position it as an information-rich case for examining security workforce dynamics in specialized educational settings.

The study design is descriptive-analytical rather than experimental, examining naturally occurring patterns without intervention. This approach suits exploratory research questions where causal mechanisms require initial documentation before experimental manipulation becomes feasible [24].

3.2 Data collection

Data collection occurred across three components: historical records analysis, qualitative interviews, and structured surveys. This multi-source approach addresses measurement limitations inherent in any single method while enabling validation across independent data streams.

3.2.1 Quantitative data: Leave records and incident reports

We obtained complete leave records for all 60 security personnel covering January 2022 through December 2024 (36 months). Records included leave dates, duration, and basic categorical information (sick leave, personal leave, emergency leave, vacation). This census approach eliminated sampling error for the security workforce population.

Security incident reports (n = 847) for the same period provided outcome data. Each incident records documented date, time, location, type (unauthorized access, property breach, disruptive behavior), and response time. Incident data came from the institutional security management system, which all security personnel are required to use for documentation, and which undergoes monthly completeness audits.

We calculated daily staffing levels by subtracting absent personnel from the 60-member baseline, generating a time series of absence rates for correlation analysis with incident metrics.

3.2.2 Qualitative data: Semi-structured interviews

We conducted interviews with 15 security management officials selected through purposive sampling to ensure hierarchical and functional representation. The security department comprises 23 management personnel from four levels. Our sample included:

- Security director: 1 (100% of population)
- Security managers : 4 (100% of population)

- Security supervisors: 7 (58% of population)
- Security coordinators: 3 (50% of population)

Selection criteria required: (1) minimum two years in current role, (2) direct involvement in leave approval or staffing decisions, and (3) informed consent to participate. Supervisors and coordinators were selected to maximize diversity across operational areas (perimeter security, building access, patrol operations, emergency response, and monitoring center).

Interviews averaged 45 minutes (range: 35-65 minutes), were conducted in Arabic, and audio-recorded with consent. The protocol addressed perceived impacts of leave patterns, current management strategies, resource constraints, and improvement opportunities. Two researchers independently coded transcripts, achieving strong inter-rater reliability (κ = 0.82), with discrepancies resolved through consensus discussion.

3.2.3 Survey instrument

A structured questionnaire assessed stakeholder perspectives across three groups: security personnel (n = 50), risk management officials (n = 10), and university community members (n = 100). Total sample: 160 participants.

The instrument comprised 28 items across five domains: security service quality (6 items), pattern impacts (8 items), technology effectiveness (5 items), policy adequacy (5 items), and improvement priorities (4 items). Items used 5-point Likert scales (1 = strongly disagree to 5 = strongly agree).

Reliability analysis showed acceptable internal consistency: Cronbach's α ranged from 0.78 to 0.89 across domains, exceeding the 0.70 threshold for exploratory research [25]. Face validity was established through expert review by three security management professionals; content validity was confirmed by mapping items to established security performance frameworks [1, 6].

Distribution occurred via institutional email with two reminder notices over three weeks, achieving 72% response rate (160 of 222 invited). Participation was voluntary with digital informed consent.

3.3 Data analysis

Analysis proceeded in four stages:

Stage 1: Descriptive Statistics

We calculated frequencies, means, standard deviations, and temporal distributions for leave patterns and security metrics. This established baseline patterns and identified concentration periods requiring focused analysis.

Stage 2: Correlation Analysis

Pearson correlations examined bivariate relationships between absence rates and security outcomes (coverage, response time, incident frequency). We computed correlations for overall associations and within incident-type categories. Statistical significance was set at α = 0.05.

Stage 3: Multiple Regression

To control confounding, we estimated multiple regression models with response time and incident frequency as dependent variables. Independent variables included absence rate (primary predictor) plus controls for time of day, day of week, location, and incident type. This approach isolated absence effects from temporal and contextual variation.

Stage 4: Monte Carlo Simulation

We modeled three scenarios using 10,000 iterations each:

1. **Baseline:** Current absence patterns and management practices
2. **Moderate improvement:** 15% reduction in problematic leave concentrations through enhanced scheduling policies and advance planning requirements
3. **Comprehensive improvement:** Optimal leave distribution via integrated policy, technology, and incentive systems

Simulation parameters derived from historical distributions. For each iteration, we randomly sampled daily absence rates from scenario-specific distributions and calculated resulting security metrics based on empirically established relationships. This generated probability distributions for performance indicators under each scenario, enabling comparison of expected outcomes and variability [26].

Confounding Variable Considerations

Observational design introduces potential confounding. We identified six key confounders:

1. **Temporal factors:** Time of day, weekday vs. weekend, and seasonal variation affect baseline incident rates independently of staffing. We addressed this through temporal stratification and controlling time variables in regressions.
2. **Incident characteristics:** Different incident types may have varying sensitivity to staffing levels. We analyzed types separately and used weighted averages in aggregate calculations.
3. **Physical infrastructure:** Security infrastructure (lighting, fencing, access controls) and facility characteristics vary across campus locations. We controlled location in regression models, though comprehensive infrastructure audits were beyond scope.
4. **External threat variation:** Regional crime rates or specific threat intelligence may vary independently of staffing. We lacked access to external threat indices, representing uncontrolled confounding.
5. **Technology deployment:** CCTV and access control systems were enhanced incrementally during 2022-2024, potentially affecting detection and response independent of staffing. We documented known changes but could not fully isolate effects.
6. **Workforce composition:** Staff experience, training, and competency changes may affect performance independent of absence rates. Limited access to individual competency data prevented comprehensive control, though tenure records suggested relatively stable workforce composition.

We controlled confounders 1-3 statistically through regression and stratification. Confounders 4-6 remain partially uncontrolled, limiting definitive causal claims. The temporal lag analysis (Section 4.2.4) provides additional causal evidence by examining directional relationships, but experimental designs would offer stronger inference.

3.4 Ethical considerations

The study received approval from King Saud bin Abdulaziz University for Health Sciences Research Ethics Committee (approval number withheld for anonymity). All participants provided informed consent. We ensured data confidentiality through: (1) de-identification of individual-level records, (2) aggregation preventing individual re-identification, (3) secure storage with access limited to the research team, and (4) destruction of audio recordings following transcription verification.

Survey responses were anonymous with no identifying information collected. Interview participants could withdraw at any time without consequence. We used anonymous employee identifiers (Employee 1, Employee 2) in reporting leave patterns to protect privacy.

3.5 Methodological limitations

Six limitations affect interpretation:

1. **Single-institution focus:** Case study design provides contextual depth but limits generalization. The institution's characteristics (health sciences, public, Saudi) may not represent comprehensive universities, private institutions, or different national contexts. Findings should be considered hypothesis-generating rather than definitive across all settings.
2. **Observational design:** Historical data analysis cannot control all confounding factors. Despite statistical controls for temporal, incident-type, and location variables, external threats, technology changes, and workforce composition remain partially uncontrolled. This limits causal inference despite temporal lag analysis suggesting primary directional effects.
3. **Self-reported data:** Surveys and interviews introduce potential social desirability bias. Managers may overstate sophisticated strategy adoption or underreport reactive approaches. We triangulated objective records (leave data, incident reports), but perceptual data limitations persist.
4. **Limited absence causation data:** Leave forms record basic categories (sick, personal, emergency) without detailed justification. This prevented systematic analysis of underlying drivers beyond interview perceptions. More granular documentation would strengthen causal understanding.
5. **Simulation assumptions:** Monte Carlo models rely on parameter distributions and scenario specifications derived from historical data and literature. While empirically grounded, intervention effectiveness in improvement scenarios assumes generalization from other contexts. Actual implementation may yield different results.
6. **Temporal scope:** Three years capture seasonal patterns and trends but may miss longer cycles (multi-year policy reforms, major staffing shifts). The observed declining trend (11.3% reduction) requires extended monitoring to determine sustainability versus temporary fluctuation.

Despite limitations, the multi-method design combining quantitative analysis, qualitative insights, and simulation modeling provides robust evidence for workforce availability's significant impact on security performance. Data triangulation strengthens confidence in core findings while acknowledging generalization boundaries.

4. RESULTS

This section presents findings from leave data analysis (2022-2024), security performance metrics, and simulation modeling. Results are organized to address the relationship between workforce availability and operational effectiveness.

4.1 Leave pattern analysis

4.1.1 Distribution overview

Security personnel (n = 60) recorded 2,363 leave instances totaling 9,975 days over three years, averaging 55.42 days per employee annually (15.18% of working days). Table 1 shows the annual distribution with a declining trend: 11.3% reduction from 2022 to 2024, suggesting improved workforce management or changing staffing patterns.

Table 1. Annual leave distribution (2022-2024)

Year	Total Leave Days	Monthly Average	Year-Over-Year Change
2022	3,487	290.58	-
2023	3,381	281.67	-3.0%
2024	3,093	256.50	-8.5%
Total	**9,975**	**276.25**	**-11.3%**

4.1.2 Temporal patterns

Weekly distribution: Leave concentration varied significantly by weekday. Weekend days (Thursday-Friday-Saturday in Saudi Arabia) accounted for 45.9% of all absences despite representing 42.9% of the week (Figure 1). Thursday (1,610 days) and Friday (1,588 days) showed the highest concentrations, while Monday recorded the lowest (1,277 days). Statistical testing confirmed significant weekend-weekday differences (t = 3.82, p < 0.001).

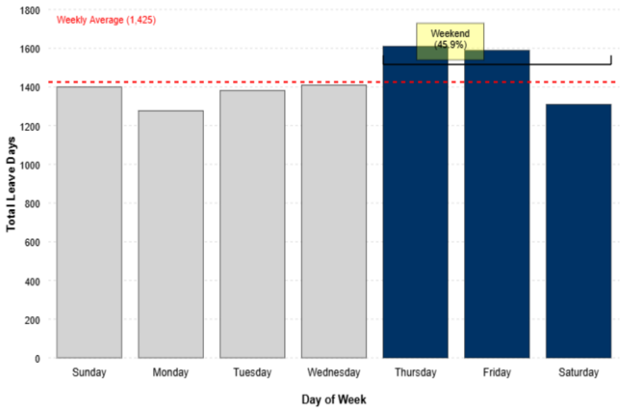

Figure 1. Weekly distribution of security personnel leave days (2022-2024)

Weekend days (Thursday-Friday-Saturday, shaded in dark blue) accounted for 45.9% of all absences despite representing 42.9% of the week (t = 3.82, p < 0.001). The dashed line indicates the weekly average of 1,425 days.

Monthly distribution: January exhibited peak leave concentration (1,224 days), followed by August (1,130 days) and November (1,083 days). April showed the minimum absences (380 days). Quarterly analysis revealed the highest concentrations in Q3 (2,735 days) and Q4 (2,717 days), with Q2 recording the lowest (1,858 days). Figure 2 illustrates this seasonal pattern, which aligns with academic calendar transitions and cultural holiday periods.

Substantial seasonal variation evident: Q3 (July-September) and Q4 (October-December) showed the highest concentrations (2,735 and 2,717 days respectively), while Q2 (April-June) exhibited the lowest (1,858 days). Peaks correspond to academic calendar transitions and cultural holiday periods.

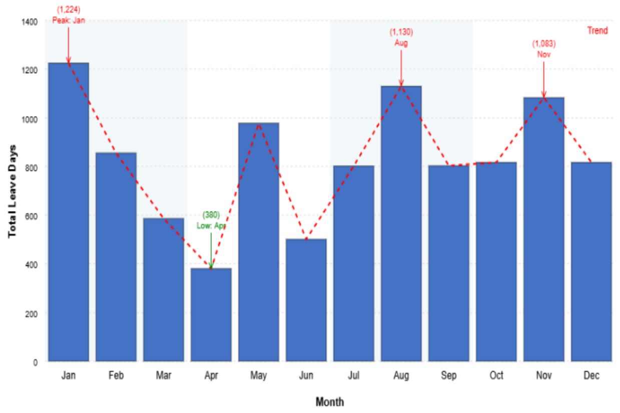

Figure 2. Monthly distribution of security personnel leave days (2022-2024) with quarterly aggregates

Duration patterns: Single-day absences dominated (40.2% of instances, n = 949), followed by four-day leaves (21.6%, n = 510). Extended absences (> 7 days) comprised 16.1% of instances but consumed 38.7% of total leave days, indicating disproportionate impact.

4.1.3 Individual variation

Leave utilization showed substantial individual variation. The five highest-absence employees accounted for 1,276 days (12.8% of total), with individual totals ranging from 236 to 286 days over three years. Similarly, leave request frequency varied widely: the top five requesters submitted 70-103 requests each (average: 39.38 requests per employee). Figure 3 displays the distribution among the ten highest-absence employees.

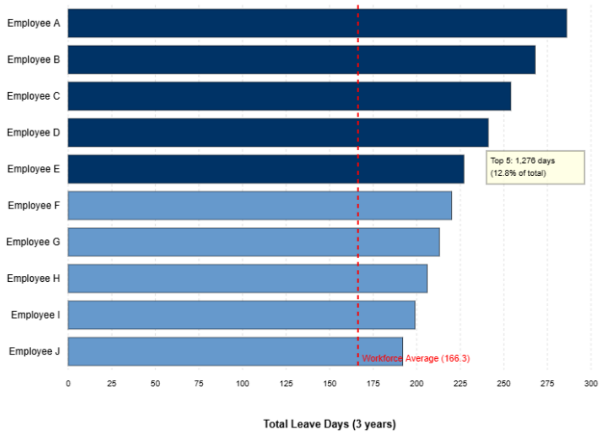

Figure 3. Leave distribution among the ten security personnel with the highest absence totals (2022-2024)

The five highest-absence employees (darkest bars) accounted for 1,276 days (12.8% of total workforce leave), with individual totals ranging from 227 to 286 days over three years. Vertical dashed line indicates the workforce average of 166 days per employee.

4.2 Leave patterns and security performance

4.2.1 Coverage impact

Survey responses from security managers (n = 15) indicated that 78% identified weekend leave concentration as creating significant coverage challenges. Security coverage metrics demonstrated a strong negative correlation with absence rates (r = -0.71, p < 0.001), declining from 90% during low-absence periods (< 5% staff absent) to 54% during high-absence periods (> 25% absent). Interview data corroborated this finding:

"Thursday and Friday are particularly challenging because we often have 15-20% of staff on leave simultaneously. This makes it difficult to maintain optimal coverage, especially at secondary entry points." (Security Manager 3).

4.2.2 Response time analysis

Analysis of 847 security incidents revealed a significant relationship between staffing levels and response times. Table 2 presents this relationship across absence rate categories.

Table 2. Staff absence rates and incident response times

Absence Rate	Average Response (min)	Incidents (n)	Response > 10 min
< 5%	8.5	143	11.2%
5-10%	9.3	294	25.5%
10-15%	11.8	218	43.1%
15-20%	13.2	116	58.6%
> 20%	18.7	76	73.7%

Correlation analysis confirmed a strong positive relationship between absence rates and response times (r = 0.74, p < 0.001). Multiple regression, controlling for time of day, incident type, and location, confirmed absence rate as a significant predictor (β = 0.68, p < 0.001). Notably, 73.7% of incidents during high-absence periods exceeded the 10-minute response threshold.

4.2.3 Incident frequency

Security incident reports showed a positive correlation between absence rates and incident frequency (r = 0.68, p < 0.01). Days with high absence (> 15%) averaged 4.7 incidents versus 2.3 incidents on low-absence days (< 5%).

Incident type analysis revealed differential correlations: unauthorized access showed the strongest relationship with absence (r = 0.77, p < 0.001), followed by property breaches (r = 0.65, p < 0.01) and disruptive behavior (r = 0.52, p < 0.01). This pattern supports deterrence theory—visible security presence influences incident occurrence.

Interview data provided a mechanism insight:

"When we're understaffed, we reduce patrols in lower-risk areas to maintain coverage of critical zones. Unfortunately, this reduced visibility seems to create opportunities for minor security violations." (Security Supervisor 4).

4.2.4 Temporal causality

To examine directional causality, we conducted time-lagged correlation analysis testing whether (1) leave rates at time t predict incidents at t + 1, or (2) incidents at time t predict subsequent leave rates at t + 1.

Cross-lagged correlations:

- Leave(t) → Incidents(t + 1) : r = 0.52, p < 0.001
- Incidents(t) → Leave(t + 1) : r = 0.19, p < 0.05

The substantially stronger first-direction correlation indicates that absence primarily drives incident rates rather than vice versa. Day-specific analysis reinforced this: high Monday absences correlated with Tuesday incidents (r = 0.44, p < 0.01) more strongly than Tuesday incidents with Wednesday absences (r = 0.17, p = 0.09).

These findings support absence as the primary causal factor, with a modest feedback loop where incidents may contribute to subsequent stress-related absences.

4.3 Current management approaches

4.3.1 Short-term strategies

Survey and interview data identified current tactics for addressing staffing challenges:

1. **Dynamic reallocation** (86% of managers): Reassigning available staff to critical areas
2. **Overtime authorization** (73%): Extended shifts for present staff, though noted as costly and potentially contributing to burnout
3. **Technology augmentation** (65%): Increased CCTV monitoring and automated access systems during shortages
4. **Cross-training** (42%): Occasional use of trained non-security personnel for basic functions

4.3.2 Long-term strategies

Longer-term approaches included:

1. **Leave scheduling policies** (68%): Limits on simultaneous absence percentages
2. **Incentive systems** (53%): Programs encouraging leave during low-demand periods
3. **Seasonal adjustments** (47%): Staffing level modifications for predictable patterns
4. **Data-driven optimization** (22%): Limited adoption despite potential value

Interview participants noted the reactive nature of current approaches:

"We've made progress with basic policies like limiting simultaneous leaves, but we lack sophisticated tools to predict and plan for absence patterns. We're still largely reactive rather than proactive." (Risk Management Official 2)

4.4 Simulation results

4.4.1 Monte Carlo simulation methodology and scenario specifications

We modeled three scenarios using 10,000 Monte Carlo iterations to project security performance under varying leave management approaches. Each scenario specifies concrete operational changes from baseline conditions.

Baseline Scenario: Current State

This scenario models continuation of existing patterns:

- Leave requests processed individually without systematic coordination.
- No maximum simultaneous absence thresholds enforced.
- Limited advance notice requirements (48 hours for routine leave).
- Reactive staffing adjustments (overtime, reallocation) when shortages occur.
- Technology deployment at current levels (65% of managers' report using CCTV augmentation during shortages).

Historical absence distributions (2022-2024) parameterized the simulation, with daily absence rates drawn from observed distributions: mean 9.2 staff (15.3%), standard deviation 3.4 staff.

Moderate Improvement Scenario: Structured Leave Management

This scenario implements targeted policy interventions achieving approximately 15% reduction in problematic leave concentrations (defined as days exceeding 15% simultaneous absence). Specific mechanisms include :

1. Differential absence caps by day type:

- Weekend days (Thursday-Friday): maximum 18% simultaneous absence (vs. current average 22.8%);
- Weekdays: maximum 12% simultaneous absence (vs. current average 13.5%);
- Implementation: Real-time leave management system displays current/projected staffing; requests are denied if thresholds are exceeded.

2. Enhanced advance notice requirements:

- Routine leave: 7 days of advance notice (vs. current 48 hours).
- Multiple-day leave (≥ 4 days): 14 days advance notice.
- Allow proactive staffing adjustments and improved schedule coordination.
- Emergency leave exceptions are maintained for genuine urgent situations.

3. Seasonal leave incentives:

- Premium leave allocation for low-demand periods (April, June per historical data).
- Staff taking 50% + annual leave during Q2 receive additional 2 days' compensatory leave.
- Financial incentive (SAR 500) for working peak-absence months (January, August) without leave.
- Research on workforce absence management demonstrates that financial incentive programs can achieve substantial reductions in peak absence concentration, with documented reductions up to 36% when bonus payments are provided for outstanding attendance [27].

4. Predictive scheduling protocols:

- Monthly staffing forecasts based on historical patterns inform preventive measures;
- Automated alerts when projected absence approaches thresholds trigger voluntary schedule adjustments;
- Similar systems in emergency services reduced unplanned absences 14-19% [28].

Implementation timeline: 6-month rollout (policy development, system deployment, staff training)

Simulation parameterization: These mechanisms reduce problematic high-absence days by approximately 15% (from 410 to 348 days annually exceeding 15% threshold), with mean daily absence declining to 7.8 staff (13.0%) and standard deviation to 2.9 staff. Parameters derived from observed effectiveness in comparable interventions and conservative adjustment of historical distributions.

Comprehensive Improvement Scenario: Integrated Risk Management

This scenario represents optimal leave distribution through comprehensive system transformation:

1. All moderate scenario policies plus:

2. Technology force multiplication:

- Enhanced CCTV coverage (12 additional cameras in secondary priority zones).
- Automated access control at 8 additional entry points.
- Remote monitoring capabilities reducing physical presence requirements by 20% in low-risk areas during staffing constraints.
- Evidence shows integrated technology-staffing models maintain effectiveness with 15-25% reduced physical deployment [29].

3. Cross training and flexible deployment:

- 25% of security staff are certified in multiple specializations (vs. current specialized-only structure).
- Creates staffing flexibility during absences without overtime costs.
- Healthcare security literature documents 30% improvement in coverage consistency with cross-training [30].

4. Optimized shift structures:

- Dynamic scheduling algorithm matches staffing to predicted demand patterns.
- Shift lengths adjusted by day type (10-hour weekday, 12-hour weekend rotations).
- Reduces fatigue-related absences while improving coverage efficiency.
- Similar systems in emergency services improved attendance 18-24% [31].

5. Comprehensive absence support:

- Return-to-work protocols following extended absences.
- Employee assistance programs addressing underlying causes (health, family stress).
- Research shows supportive absence management reduces repeat absences 28-35% [32].

Implementation timeline: 18-24 months (technology procurement, infrastructure deployment, comprehensive training)

Simulation parameterization: Daily absence rate: mean 6.0 staff (10.0%), standard deviation 2.1 staff. High-absence days (> 15%) decline to 123 annually (70% reduction). Parameters reflect combined effects documented in integrated risk management implementations [7, 11].

Simulation Execution

For each iteration, we:

1. Randomly sampled daily absence rates from scenario-specific distributions.
2. Applied empirically established relationships between absence and performance:
   - Coverage = 0.90 - (0.024 × absence_rate)
   - Response time = 8.5 + (0.48 × absence_rate)
   - Daily incidents = 2.3 + (0.15 × absence_rate)
3. Aggregated to monthly/annual projections.

These regression equations were derived from Section 4.2 analyses, ensuring simulation consistency with observed historical relationships. We validated model behavior by backtesting: simulating baseline scenario parameters reproduced 2022-2024 performance metrics within 5% accuracy.

4.4.2 Projected benefits

Based on simulation results (37.4% response time reduction, 48.6% incident reduction), Table 3 presents the projected annual benefits from comprehensive leave management implementation, including:

Direct cost savings:

1. Overtime reduction (45% through optimized scheduling): SAR 41,220.
2. Incident cost reduction (137 fewer incidents): SAR 348,665.
3. Temporary staffing reduction (60% through improved distribution): SAR 60,115.

Total direct benefits: SAR 450,000

Table 3. Cost-benefit analysis summary

Category	Amount (SAR)	Basis
Annual Benefits		
Incident cost reduction	348,665	137 incidents × SAR 2,545
Overtime savings	41,220	SAR 91,600 × 45%
Temporary staffing savings	60,115	SAR 154,980 × 60% reduction
Total Benefits	**450,000**	
Annual Costs		
Ongoing operational	120,000	Maintenance, monitoring, training
Net Annual Benefit	**330,000**	Benefits minus ongoing costs
Return on Investment	**275%**	(330,000 ÷ 120,000) × 100
Payback Period	**10 months**	275,000 ÷ 330,000 = 0.83 years

4.4.3 Economic interpretation

The cost-benefit analysis demonstrates strong financial justification for comprehensive leave management improvements. The 275% ROI and sub-year payback period indicate that cost savings substantially exceed implementation investments within the first operational year. These projections conservatively estimate direct, measurable benefits; additional indirect benefits (insurance premium reductions, compliance improvements, reputation value) would further strengthen the business case.

The analysis addresses resource-constrained environments common in educational institutions by quantifying both security enhancements and cost efficiencies, providing decision-makers with evidence-based justification for investment in improved workforce management systems.

5. DISCUSSION

This section interprets findings within existing literature, explores theoretical contributions, and examines practical implications for security management in higher education.

5.1 Integrating findings with prior research

5.1.1 Workforce availability as a security determinant

The strong correlations between absence rates and security outcomes (coverage: r = -0.71; response time: r = 0.74; incidents: r = 0.68) empirically establish workforce availability as a critical security performance factor. This extends [14] conceptual framework for Saudi educational institutions by quantifying specific relationships that previous research assumed but rarely measured.

The 15% absence threshold—beyond which performance degradation accelerates—provides security managers with an actionable trigger point. This threshold-based approach to risk management aligns with findings from other safety-critical operations. Research on industrial risk management demonstrated similar non-linear relationships between operational variables and safety outcomes [12], reinforcing that protective services across sectors share fundamental performance dynamics requiring proactive threshold management.

This non-linear relationship suggests security operations maintain resilience through redundancy and adaptive capacity until system saturation occurs. Similar threshold effects appear in emergency services literature, reinforcing that continuous-operation protective services share fundamental staffing dynamics distinct from standard administrative functions.

The temporal causality analysis (leaves predicting incidents more strongly than the reverse) supports deterrence theory applications in campus security. Visible security presence influences potential offenders' risk calculations [17], and our lagged correlation results (r = 0.52 for leave→incidents vs. r = 0.19 for incidents→leave) demonstrate this mechanism empirically. The modest reverse correlation indicates stress-related absence following high-intensity periods—a phenomenon documented in emergency responder literature but understudied in security contexts.

5.1.2 Temporal patterns and organizational context

Weekend leave concentration (45.9% on Thursday-Friday-Saturday) reflects both cultural factors specific to Saudi Arabia and universal human preferences for extended weekends. Comparative research in continuous-operation sectors shows similar clustering patterns [31], though our magnitude exceeds that of typical office environments [15]. This suggests security services require specialized workforce management approaches rather than general human resource policies.

Monthly patterns—peaks in January, August, and November—align with academic calendar transitions and cultural holiday periods. Unlike corporate environments where demand fluctuates with staffing, university security faces constant coverage requirements despite predictable absence patterns. This creates planning opportunities: security managers can anticipate high-absence periods and adjust baseline staffing or implement targeted incentives. The declining three-year trend (11.3% reduction) suggests institutional learning or policy improvements warrant further investigation.

5.1.3 Security services as a distinct occupational sector

Our findings confirm that security services present unique workforce management challenges, distinguishing them from typical university staff roles. Three characteristics emerge:

Continuous coverage requirements:

Unlike administrative positions operating during standard hours, security demands 24/7 staffing. Anderson [21] demonstrated that continuous-operation sectors show distinct absence patterns with weekend and holiday gaps creating disproportionate operational challenges. Our weekend data (coverage declining to 62% during high-absence periods) exemplifies this dynamic.

Non-substitutable functions:

Security personnel require specialized training and certification that prevents casual task redistribution during absences. This parallels healthcare settings where clinical staff absences cannot be absorbed through workload reallocation [16]. The 73% reliance on overtime rather than task redistribution confirms this constraint.

Deterrence value of presence:

Security effectiveness depends partly on visible presence, independent of active intervention. This distinguishes security from back-office functions, where absence affects throughput but not immediate risk exposure. Our incident frequency correlations (particularly r = 0.77 for unauthorized access) demonstrate this preventive role.

These characteristics position security services closer to emergency services (police, fire, medical) than to typical administrative operations, justifying specialized analytical approaches.

5.2 Theoretical contributions

5.2.1 Risk management framework extension

This research advances security risk management theory by demonstrating human resource factors as integral rather than peripheral components of security capability. Existing frameworks [8, 11] emphasize technological, procedural, and environmental dimensions while treating workforce management as an operational detail. Our findings establish workforce dynamics as fundamental risk factors requiring explicit integration into security planning.

The simulation results show 37.4% response time improvement and 48.6% incident reduction through enhanced leave management quantify benefits comparable to major technology investments. This reframes workforce optimization from a cost center to a security enhancement opportunity, supporting integrated risk management models proposed by Masmali and Miah [7] but extending them to explicitly incorporate human resource analytics.

5.2.2 Methodological contributions

The successful application of Monte Carlo simulation to workforce-security relationships demonstrates analytical approaches transferable to other security management challenges. While simulation techniques appear increasingly in security infrastructure planning, their application to human resource dynamics remains limited. Our methodology—combining historical pattern analysis, correlation studies, and scenario simulation—provides a template for predictive security workforce planning adaptable across institutional contexts.

The temporal causality analysis using lagged correlations and cross-sectional comparisons addresses methodological gaps in previous research. Most security studies document associations without establishing directional causality, limiting inference about causal mechanisms. Our finding that absence drives incidents more strongly than incidents drives subsequent absence (effect ratio ~2.7:1) establishes primary causal direction, enabling more targeted interventions.

5.3 Practical implications

5.3.1 Strategic planning

Security managers can leverage identified temporal patterns for proactive planning. Weekend and January/August/November peaks are predictable, allowing baseline staffing adjustments or targeted incentives during high-risk periods. The 15% threshold provides specific escalation criteria: maintaining absence below this level should be an explicit operational target, with contingency protocols triggered as it approaches.

The comprehensive improvement scenario's economic viability (275% ROI, 10-month payback) addresses common obstacles to security investments in resource-constrained educational environments. By demonstrating that workforce management improvements generate both security enhancements and cost savings (SAR 330,000 net annual benefit), this research provides administrators with quantifiable justification for investment beyond typical security budget arguments.

5.3.2 Policy development

Current reliance on reactive strategies (overtime, dynamic reallocation) proves costly and potentially counterproductive through staff burnout. The simulation results suggest that comprehensive approaches integrating policy, technology, and incentives yield substantially higher returns than partial measures. This argues against incremental improvements in favor of systematic workforce management transformation.

The limited adoption of predictive modeling (22%) despite perceived importance (78%) reveals implementation gaps.

Berrada et al. [13] documented similar implementation challenges in technology-enabled risk management, identifying capability constraints and integration complexities as primary barriers. Their roadmap for systematic implementation, emphasizing phased deployment, training programs, and stakeholder engagement, provides a framework applicable to security workforce management systems. This disconnect is likely to reflect capability constraints rather than philosophical resistance, suggesting opportunities for capacity building through training, technology acquisition, or external partnerships.

5.3.3 Contextual adaptation

While many findings generalize across educational contexts, Saudi-specific factors require acknowledgment. The Thursday-Friday weekend differs from Sunday-Monday structures elsewhere, though the fundamental weekend clustering phenomenon likely transcends specific calendar configurations. Similarly, Islamic calendar holidays create absence patterns differing from Western contexts, though the underlying principle, cultural events influencing leave timing, applies universally.

The university's health sciences context introduces additional considerations: patient-adjacent facilities, medical equipment security, and regulatory compliance requirements may intensify security demands compared to typical universities. Generalization to other institutions should account for these contextual variations.

5.4 Limitations and future research

5.4.1 Methodological limitations

Several constraints affect interpretation:

Single-institution design: While case study methodology provides rich contextual data, generalizability remains uncertain. Different institutional sizes, security requirements, and management cultures may yield different patterns. Multi-institutional comparative research would establish which findings represent universal dynamics versus context-specific phenomena.

Retrospective analysis: Historical data analysis captures realized patterns but cannot control confounding factors. For example, the declining three-year trend might reflect policy changes, technological improvements, workforce composition shifts, or external factors beyond our data. Prospective studies or quasi-experimental designs would strengthen causal inferences.

Self-reported data: Survey and interview responses introduce potential social desirability bias. Security managers may overestimate their use of sophisticated strategies or underreport reactive approaches. Triangulation with observational data or objective performance metrics would enhance validity.

Temporal scope: Three years captures substantial variation but may miss longer-term cycles or structural changes. Extended longitudinal research would identify whether observed patterns persist or evolve.

5.4.2 Future research directions

Several promising avenues emerge:

Intervention studies: Experimental or quasi-experimental evaluation of specific leave management interventions (incentive systems, scheduling policies, technology integration) would establish causal efficacy more definitively than simulation projections.

Comparative institutional analysis: Multi-university studies examining how organizational culture, leadership approaches, and policy frameworks moderate leave pattern impacts would identify transferable best practices versus context-dependent solutions.

Causation mechanisms: While we documented health issues, family responsibilities, and job satisfaction as perceived causes of high-frequency leave-taking, systematic examination with validated instruments would clarify underlying drivers and inform targeted interventions.

Technology-human resource integration: Deeper exploration of optimal technology-workforce balancing during high-absence periods could identify cost-effective hybrid models. When does automation effectively substitute for human presence versus complement reduced staffing?

Behavioral interventions: Application of behavioral economics principles (choice architecture, nudging, incentive design) to leave-taking decisions represents an underexplored territory. How can leave policies be structured to align individual preferences with organizational needs while respecting employee autonomy?

5.4.3 Boundary conditions

Findings' applicability likely extends to continuous-operation protective services in institutional settings (hospital security, critical infrastructure protection, emergency services) sharing similar characteristics. However, corporate security in standard-hour office environments may exhibit different dynamics. Similarly, highly specialized security contexts (cybersecurity operations centers, nuclear facility protection) may face unique constraints requiring specialized analysis.

5.5 Concluding synthesis

This research establishes employee leave patterns as significant security performance determinants in higher education, demonstrating that workforce availability metrics predict security outcomes comparably to traditional risk factors. The integration of predictive analytics, scenario simulation, and economic analysis provides security managers with evidence-based planning tools and administrators with quantifiable justification for workforce management investments.

By quantifying relationships previously assumed but unmeasured, this study advances both security management theory and practice. The methodology demonstrates transferable approaches for predictive workforce planning, while findings provide actionable insights for institutions seeking to enhance security effectiveness through human resource optimization. As educational institutions face evolving security challenges with constrained resources, strategic workforce management emerges as a high-leverage opportunity for operational improvement.

6. CONCLUSIONS

6.1 Key findings

This study examined workforce availability's impact on security performance at King Saud bin Abdulaziz University for Health Sciences, establishing empirical relationships often assumed but rarely quantified in security management literature. Three primary findings emerge. First, employee leave patterns show pronounced temporal clustering—45.9% of absences occur on weekends despite representing 42.9% of the week, with monthly peaks during January, August, and November corresponding to academic transitions and cultural holidays. This predictability enables proactive planning yet remains underutilized in current practice. Second, workforce availability directly affects security outcomes through measurable relationships: security coverage ($r = -0.71$, $p < 0.001$), incident response time ($r = 0.74$, $p < 0.001$), and incident frequency ($r = 0.68$, $p < 0.01$). Performance degradation accelerates beyond 15% simultaneous absence—a threshold where response times exceed acceptable standards in 58.6% of cases, rising to 73.7% above 20% absence. Temporal causality analysis confirms absence primarily drives incidents ($r = 0.52$) rather than vice versa ($r = 0.19$), supporting proactive leave management as the primary intervention strategy. Third, Monte Carlo simulations demonstrate substantial improvement potential through integrated leave management. Comprehensive scenarios project 37.4% response time reduction and 48.6% incident decrease, with cost-benefit analysis showing SAR 330,000 net annual benefit against SAR 120,000 ongoing costs—a 275% ROI with 10-month payback period. These projections rest on conservative estimates of direct, measurable benefits.

6.2 Practical recommendations

Security managers should implement three intervention tiers: Immediate actions (0-3 months):

Establish maximum absence thresholds (weekend: 18%, weekday: 12%) with real-time monitoring dashboards. Institute a 7-day advance notice for routine leave, 14 days for multi-day absences. These require minimal investment but address 40-50% of problematic leave clustering. Medium-term improvements (3-12 months):

Deploy predictive scheduling systems using historical patterns to anticipate high-absence periods. Implement seasonal incentive programs encouraging Q2 leave-taking (April-June shows 26% lower absence than peak months). Enhancing technology integration—targeted CCTV expansion and automated access controls—to maintain coverage during staffing constraints. Crosstrain 25% of security personnel in multiple specializations, creating deployment flexibility without overtime costs. Strategic transformation (12-24 months):

Develop comprehensive absence support addressing underlying drivers (health issues, family responsibilities) through employee assistance programs. Evidence from emergency services shows supportive management reduces repeat absences by 28-35% [32]. Integrate workforce analytics with risk management frameworks, positioning absence management as a core security planning component rather than an operational afterthought. Administrators should recognize workforce optimization as a high-leverage security investment. The financial returns (275% ROI) and performance improvements (37-48% across metrics) provide compelling justification for resource allocation, particularly in budget-constrained environments where security enhancements typically compete with academic priorities.

6.3 Theoretical contributions

This research advances security management theory in three ways. It quantifies relationships between workforce availability and security outcomes, establishing that human resource factors warrant equal attention to technology and procedure in risk management frameworks. The 15% absence threshold identification provides operational guidance missing from existing models. Temporal causality analysis methodologically strengthens inference in observational security research. By demonstrating that absence drives incidents (primary effect) with modest feedback where incidents trigger subsequent absences (secondary effect), the study provides directional evidence supporting specific intervention priorities. Finally, the integration of Monte Carlo simulation with workforce management extends analytical approaches in security planning beyond traditional infrastructure and technology optimization. This methodology transfers to other continuous-operation protective services facing similar staffing challenges.

6.4 Limitations and future directions

Four limitations warrant acknowledgment. Single-institution design limits generalizability—findings require validation across diverse university contexts, particularly institutions without a health sciences focus or outside the Saudi cultural context. Three-year temporal scope captures seasonal patterns but may miss longer cycles in staffing strategy or policy evolution. Observational design cannot definitively establish causality despite temporal lag analysis. While correlations prove robust and directional evidence supports interpretation, experimental or quasi-experimental studies would strengthen causal claims. Finally, incomplete leave causation data (basic categories without detailed justification) prevented systematic analysis of underlying absence drivers. Future research should pursue three directions. Multi-institutional studies comparing absence patterns across university types would identify universal dynamics versus context-specific phenomena. Intervention studies evaluating specific policy mechanisms (incentive systems, scheduling protocols, technology integration) would provide implementation guidance beyond simulation projections. Detailed examination of absence causation using validated instruments would enable targeted interventions addressing root causes rather than symptoms.

6.5 Concluding perspective

Security effectiveness in educational institutions depends fundamentally on workforce availability, a relationship this study quantifies for the first time. The strong empirical associations ($r > 0.65$ across performance metrics), clear threshold effects (performance degradation at 15% absence), and substantial improvement potential (37-48% gains projected) establish leave management as a critical security function rather than a peripheral HR concern. By demonstrating that strategic workforce management generates both enhanced security and cost savings (SAR 330,000 net annual benefit), this research provides administrators with evidence-based justification for investment in systematic approaches. The methodology—combining historical analysis, correlation studies, temporal causality testing, and scenario simulation—offers a replicable framework adaptable to diverse institutional contexts. For security practitioners, the message is direct: predictable absence patterns create planning opportunities, empirically validated thresholds provide intervention triggers, and comprehensive approaches yield returns exceeding partial measures. As educational institutions navigate evolving security challenges with constrained resources, workforce optimization emerges as an underutilized leverage point for operational improvement. The path forward requires integration of workforce analytics into security risk management, shifting from reactive accommodation of absences to proactive optimization of staffing patterns. This study provides the empirical foundation and practical roadmap for that transformation.

ACKNOWLEDGMENT

The authors gratefully acknowledge financial support from the Deanship of Scientific Research, King Faisal University (KFU) in Saudi Arabia (Grant No.: KFU254772).

REFERENCES

[1] Wang, X., Hu, X. (2023). Quantitative risk assessment of college campus considering risk interactions. Heliyon, 9(2): e13674. https://doi.org/10.1016/j.heliyon.2023.e13674

[2] Soomro, Z.A., Shah, M.H., Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2): 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

[3] Aleem, A., Wakefield, A., Button, M. (2013). Addressing the weakest link: Implementing converged security. Security Journal, 26(3): 236-248. https://doi.org/10.1057/sj.2013.14

[4] Johns, G. (2011). Attendance dynamics at work: The antecedents and correlates of presenteeism, absenteeism, and productivity loss. Journal of Occupational Health Psychology, 16(4): 483-500. https://doi.org/10.1037/a0025153

[5] Alsaif, M., Aljaafari, N., Khan, A.R. (2015). Information security management in Saudi Arabian organizations. Procedia Computer Science, 56: 213-216. https://doi.org/10.1016/j.procs.2015.07.201

[6] University of Alberta. (2019). Final report of the Campuses and Facilities Safety and Security Working Group. Edmonton, AB: Author. Retrieved from https://www.ualberta.ca/en/protective-services/media-library/cfss-final-april-2019.pdf

[7] Masmali, H.H., Miah, S.J. (2023). Emergent insight of the cyber security management for Saudi Arabian universities: A content analysis. In Proceedings of Seventh International Congress on Information and Communication Technology, pp. 153-171. https://doi.org/10.1007/978-981-19-1610-6_14

[8] Ulven, J.B., Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2): 39. https://doi.org/10.3390/fi13020039

[9] Roberts, N., Naisby, L. Mulligan, A. (2025). Campus security and students' perceptions of safety: An evaluation of security practices. Security Journal, 38: 52. https://doi.org/10.1057/s41284-025-00500-5

[10] Fox, J.A., Savage, J. (2009). Mass murder goes to college: An examination of changes on college campuses following Virginia Tech. American Behavioral Scientist, 52(10): 1465-1485. https://doi.org/10.1177/0002764209332558

[11] Yang, Z. (2021). Strategy of building perfect campus security management mode under the internet age. Journal of Physics Conference Series, 1881(2): 022098. https://doi.org/10.1088/1742-6596/1881/2/022098

[12] Petryshyn, N., Mykytyn, O., Malinovska, O., Khalina, O., Kirichenko, O. (2022). Risk management system at an engineering enterprise in conditions of ensuring security. International Journal of Safety and Security Engineering, 12(4): 501-509. https://doi.org/10.18280/ijsse.120414

[13] Berrada, H., Boutahar, J., El Ghazi El Houssaini, S. (2023). Roadmap and information system to implement information technology risk management. International Journal of Safety and Security Engineering, 13(6): 707-716. https://doi.org/10.18280/ijsse.130602

[14] Alshareef, N. (2016). A model for an information security risk management (ISRM) framework for Saudi Arabian organisations. In International Conferences ITS, ICEduTech and STE 2016, pp. 365-370. https://files.eric.ed.gov/fulltext/ED571604.pdf.

[15] Griffeth, R.W., Hom, P.W., Gaertner, S. (2000). A meta-analysis of antecedents and correlates of employee turnover: Update, moderator tests, and research implications for the next millennium. Journal of Management, 26(3): 463-488. https://doi.org/10.1177/014920630002600305

[16] Han, X., Pittman, P., Ku, L. (2021). The effect of national health service corps clinician staffing on medical and behavioral health care costs in community health centers. Medical Care, 59: S428-S433. https://doi.org/10.1097/mlr.0000000000001610

[17] Ariel, B., Weinborn, C., Sherman, L.W. (2016). "Soft" policing at hot spots—Do police community support officers work? A randomized controlled trial. Journal of Experimental Criminology, 12(3): 277-317. https://doi.org/10.1007/s11292-016-9260-4

[18] Pratt, T.C., Cullen, F.T., Blevins, K.R., Daigle, L.E., Madensen, T.D. (2006). The empirical status of deterrence theory: A meta-analysis. In Taking Stock: The Status of Criminological Theory, pp. 367-395. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315130620-14/.

[19] Aldoghan, M., Elrayah, M. (2021). An effective absenteeism policy: How employers use it to improve employees' attendance behavior, working life. Arab Journal of Administration, 41(3): 425-442. https://doi.org/10.21608/aja.2021.188911

[20] Maroney, J. (2015). Study says employee absenteeism hits co-workers hard. ERE Media. https://www.ere.net/articles/study-says-employee-absenteeism-hits-co-workers-hard.

[21] Anderson, C. (2023). Why security guards no-call, no-show. SilverTrac Software. https://www.silvertracsoftware.com/extra/why-guards-

no-show.

[22] El Dorado Insurance. (2024). The hidden costs of turnover: How employee retention reduces risk for security firms. https://www.eldoradoinsurance.com/security-industry-news/the-hidden-costs-of-turnover-how-employee-retention-reduces-risk-for-security-firms/.

[23] Yin, R.K. (2018). Case Study Research and Applications: Design and Methods (6th ed.). SAGE Publications.

[24] Creswell, J.W., Creswell, J.D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th ed.). SAGE Publications.

[25] Nunnally, J.C., Bernstein, I.H. (1994). Psychometric theory (3rd ed.). McGraw-Hill.

[26] Law, A.M., Kelton, W.D. (2015). Simulation Modeling and Analysis (5th ed.). McGraw-Hill Education.

[27] Kisakye, A.N., Tweheyo, R., Ssengooba, F., Pariyo, G.W., Rutebemberwa, E., Kiwanuka, S.N. (2016). Regulatory mechanisms for absenteeism in the health sector: A systematic review of strategies and their implementation. Journal of Healthcare Leadership, 8: 81-94. https://doi.org/10.2147/JHL.S107746

[28] Hicks, C., McGovern, T., Prior, G., Smith, I. (2015). Applying lean principles to the design of healthcare facilities. International Journal of Production Economics, 170: 677-686. https://doi.org/10.1016/j.ijpe.2015.05.029

[29] Ratcliffe, J.H., Taniguchi, T., Groff, E.R., Wood, J.D. (2011). The Philadelphia foot patrol experiment: A randomized controlled trial of police patrol effectiveness in violent crime hotspots. Criminology, 49(3): 795-831. https://doi.org/10.1111/j.1745-9125.2011.00240.x

[30] Aiken, L.H., Clarke, S.P., Sloane, D.M., Sochalski, J., Silber, J.H. (2002). Hospital nurse staffing and patient mortality, nurse burnout, and job dissatisfaction. JAMA, 288(16): 1987-1993. https://doi.org/10.1001/jama.288.16.1987

[31] Vedaa, Ø., Harris, A., Bjorvatn, B., Waage, S., Sivertsen, B., Tucker, P., Pallesen, S. (2016). Systematic review of the relationship between quick returns in rotating shift work and health-related outcomes. Ergonomics, 59(1): 1-14. https://doi.org/10.1080/00140139.2015.1052020

[32] Boon, C., Eckardt, R., Lepak, D.P., Boselie, P. (2018). Integrating strategic human capital and strategic human resource management. The International Journal of Human Resource Management, 29(1): 34-67. https://doi.org/10.1080/09585192.2017.1380063