**CBEL Journal of Multidisciplinary Research**
Vol. 1 No. 1 (2026): ISSN (Online): 3108-8848
DOI: https://doi.org/10.66313/m7r6z835
*Socio-Technical Analysis of the Awareness–Behaviour Gap in Higher Education Cybersecurity: Evidence from Tanzania*

# Socio-Technical Analysis of the Awareness-Behaviour Gap in Higher Education Cybersecurity: Evidence from Tanzania

**Daniel John Temu[1] Joseph Chrisant Pengo[2] & Isaac Lauden Mugogo[3]**
*[1&3]Department of Information and Communication Technology, The Mwalimu Nyerere Memorial Academy (MNMA), Tanzania*

*[2]Department of Computing and Communication Technology, National Institute of Transport (NIT), Tanzania*

**Corresponding author: djitemu@gmail.com*

ORCID
Daniel John Temu https://orcid.org/0000-0001-7226-517X

**Article History**
*Received: 2026-05-20*
*Revised: 2026-06-30*
*Accepted: 2026-07-22*
*Published: 2026-07-31*

***Keywords***
Information systems security, Cybersecurity awareness, Security behaviour, Awareness–behaviour gap, Higher learning institutions

**How to cite:**
Temu, D. J., Pengo, J. C., & Mugogo, I. L. (2026). Socio-Technical Analysis of the Awareness–Behaviour Gap in Higher Education Cybersecurity: Evidence from Tanzania. *CBEL Journal of Multidisciplinary Research*, *1*(1), 63-78. https://doi.org/10.66313/m7r6z835

**Abstract**
The increasing reliance on digital systems in higher learning institutions has introduced significant information security challenges, particularly those associated with human behaviour. This study examines the socio-technical dimensions of the awareness–behaviour gap in information systems security at Mwenge Catholic University (MWECAU). Employing a mixed-methods case study design guided by the Theory of Planned Behaviour (TPB) and the Knowledge–Attitude–Behaviour (KAB) model, the study investigates how cybersecurity awareness translates or fails to translate into secure user behaviour, while simultaneously assessing system-level technical vulnerabilities using OWASP ZAP version 2.12.0. Data were collected from 65 staff members at MWECAU using structured questionnaires and key informant interviews, alongside a technical vulnerability assessment conducted using OWASP ZAP. The findings reveal a moderate overall Information Systems Security Awareness (ISSA) score of 70% (Knowledge: 68.2%; Behaviour: 71.9%; Attitude: 70.4%), computed using the Kruger and Kearney (2006) weighted formula. While most participants demonstrated positive attitudes toward information security. However, secure practices were inconsistent, indicating a clear gap between knowledge and behaviour. Notably, 66.2% of respondents had not received formal training, and only 33.8% were aware of institutional security policies. The system assessment further revealed vulnerabilities such as application error disclosures and internal IP leakage. The study concludes that awareness alone is insufficient to ensure secure behaviour. The awareness–behaviour gap is driven by a confluence of inadequate formal training, weak policy communication, limited enforcement mechanisms, and identifiable technical vulnerabilities in the institutional MIS. The findings contribute to the socio-technical understanding of cybersecurity in resource-constrained higher education environments and offer actionable recommendations for bridging the gap between knowledge and practice through integrated human and technical security strategies.

CBEL Journal of Multidisciplinary Research
Vol. 1 No. 1 (2026): ISSN (Online): 3108-8848
DOI: https://doi.org/10.66313/m7r6z835
*Socio-Technical Analysis of the Awareness–Behaviour Gap in Higher Education Cybersecurity: Evidence from Tanzania*

## INTRODUCTION

In recent years, higher learning institutions (HLIs) have experienced rapid digital transformation. Universities now depend heavily on Information and Communication Technologies (ICT) to support teaching, learning, research, and administrative activities. Systems such as Management Information Systems (MIS) are used to manage student records, examination results, staff information, and financial data. These systems have made university operations faster and more efficient. However, as institutions become more digital, they also become more exposed to cybersecurity risks. Sensitive information stored in these systems can be targeted by attackers, making information security a major concern for universities today (Zwilling et al., 2020).

To address these risks, many institutions invest in technical security solutions such as firewalls, antivirus software, encryption, and intrusion detection systems. While these tools are important, they do not fully solve the problem. Research shows that many security incidents are not caused by system failures, but by human actions. In other words, people are often the weakest link in information security (Triplett, 2022). For example, users may create weak passwords, share login credentials, click on suspicious links, or ignore security warnings. These everyday actions can open the door to cyberattacks, even when strong technical controls are in place.

This challenge is especially visible in university environments. Universities are designed to be open and collaborative spaces where information is shared freely among students, lecturers, and administrators. While this openness supports learning and innovation, it also makes it harder to enforce strict security controls. As a result, universities are often seen as easy targets for cybercriminals. Studies have shown that cyberattacks in educational institutions frequently exploit human weaknesses, such as lack of awareness or poor security practices (Nifakos et al., 2021).

Because of this, Information Systems Security Awareness (ISSA) has become an important area of focus. ISSA refers to how well users understand information security risks, how they feel about them, and how they behave in response. It includes three key aspects: knowledge (what users know about security), attitude (how they think about security), and behaviour (what they actually do in practice). Improving ISSA is seen as a cost-effective way to reduce security risks, especially in environments where resources are limited.

However, improving awareness alone is not enough. Many studies have found that there is often a gap between what people know and what they actually do. For example, a staff member may understand that passwords should be strong and unique, but still reuse the same password across multiple systems. Similarly, users may know that phishing emails are dangerous but still click on suspicious links. This disconnect between awareness and action is known as the awareness–behaviour gap (Amoresano & Yankson, 2023; Zwilling et al., 2020). It shows that knowledge does not always lead to secure behaviour.

To better understand this gap, researchers often use behavioural theories. One of the most widely used is the Theory of Planned Behaviour (TPB), developed by Ajzen (1991). According to this theory, a person's behaviour is influenced by three main factors: their attitude toward the behaviour, the social pressure they feel (subjective norms), and their perceived ability to perform the behaviour (perceived behavioural control). In the context of information security, this means that even if users have a positive attitude toward security, they may still fail to act securely if they feel unsupported or lack the necessary skills.

Recent studies in higher education support this idea. For instance, research has shown that students and staff often have moderate awareness of cybersecurity issues but still engage in unsafe practices due to limited training and weak institutional support (Goliath et al., 2024; Parikh & Nimbekar, 2023; Temu, 2017). Other studies also highlight that knowledge, attitude, and behaviour are closely related, but improvements in one area do not automatically lead to improvements in the others (Alam et al., 2024). This suggests that addressing cybersecurity challenges requires more than just awareness campaigns; it requires a deeper understanding of human behaviour.

In developing countries such as Tanzania, the situation is even more challenging. Many higher learning institutions operate with limited financial and technical resources. This can affect their ability to invest in advanced security technologies and continuous training programs. Although there are national laws and policies, such as the Cybercrimes Act of 2015, their implementation at the institutional level is often weak (Chacha et al., 2024; Sife, 2022). In some cases, security policies exist but are not well communicated to staff or students (Hina et al., 2020). As a result, users may not even be aware of the rules they are expected to follow.

At the same time, technical vulnerabilities in institutional systems can increase the risk of cyberattacks. Without regular system updates, security testing, and monitoring, weaknesses in software and networks can go unnoticed (Alkhazi et al., 2022; Chacha et al., 2024). When these technical weaknesses are combined with low user awareness, the overall security risk becomes even higher. This shows that information security is not just a technical issue or a human issue; it is a combination of both.

Despite the importance of this issue, many previous studies (e.g., Alharbi & Tassaddiq, 2021; Hong et al., 2022; Moletsane & Tsibolane, 2020) have focused on either human factors or technical vulnerabilities, but not both together. This creates a gap in understanding how these two aspects interact in real-world settings. For example, it is not enough to know that users lack awareness; it is also important to understand how this lack of awareness relates to actual system weaknesses. Similarly, identifying technical vulnerabilities without considering user behaviour provides only a partial picture of the problem.

This study aims to address this gap by examining both human and technical aspects of information systems security in a Tanzanian higher learning institution. It focuses on understanding the relationship between security awareness and actual behaviour, as well as identifying system-level vulnerabilities. By framing this relationship as an awareness–behaviour gap, the study provides a more complete view of the challenges facing universities. The findings of this study are expected to contribute to both theory and practice. From a theoretical perspective, the study adds to the growing body of knowledge on human-centred cybersecurity, particularly in the context of developing countries. From a practical perspective, it offers insights that can help universities design more effective security strategies. These may include improving training programs, strengthening policy enforcement, and integrating technical and human-focused approaches to cybersecurity.

In today's digital world, securing information systems is not just about technology, it is about people, behaviour, and culture. Understanding how these elements interact is essential for building safer and more resilient higher learning institutions.

## METHODOLOGIES

### Research Paradigm and Design

This study utilised an epistemological positivist paradigm, which prioritises objective measurement and empirical evidence. The adoption of this paradigm aligns with cybersecurity research, where quantifiable variables such as awareness levels, behaviour patterns, and system vulnerabilities are often analyzed statistically to establish relationships and draw generalizable conclusions (Creswell & Creswell, 2018). A descriptive case study design was employed to provide an in-depth analysis of a specific institutional context. The selection of a case study design was motivated by the need to explore contemporary cybersecurity phenomena within their real-life context, specifically, how a functioning Tanzanian university manages the tension between data accessibility and data security. Case study approaches have been widely used in cybersecurity research to capture contextual and organisational dynamics that cannot be easily isolated in experimental settings (Hong et al., 2022).

A mixed-methods approach was integrated to provide methodological triangulation. By comparing quantitative survey results with qualitative interview insights and empirical technical scans, the researcher ensured that the findings were not dependent on a single data source. This approach is particularly valuable in cybersecurity studies, as it allows the integration of technical system evidence with human behavioural factors. Prior studies emphasize that effective cybersecurity analysis requires both technical assessment and human-centred evaluation to fully understand system risks and user behaviour (Zwilling et al., 2020; Alkhazi et al., 2022).

## Study Area and Population

The research was conducted at MWECAU. This site was selected as it represents a typical growing academic environment with an integrated Management Information System (MIS) but without a fully matured, dedicated Security Operations Center (SOC). Such environments are common in developing countries, where digital transformation often progresses faster than the implementation of comprehensive cybersecurity frameworks. The target population consisted of 186 employees, comprising academic staff responsible for research and grading data, and administrative staff responsible for financial and personnel records. These groups were selected because they are primary users of institutional systems and play a direct role in handling sensitive information. Previous studies in higher education have similarly focused on staff and students as key actors influencing information security outcomes (Alharbi & Tassaddiq, 2021).

## Sample Size and Sampling Techniques

Using the Slovin formula ($n = N/(1 + Ne^2)$) at a 90% confidence level ($margin\ of\ error\ e = 0.10$), a sample size of 65 was determined from a target population of $N = 186$ registered MIS users. The computation was as follows: $n = 186 / (1 + 186 \times 0.10^2) = 186 / (1 + 1.86) = 186 / 2.86 \approx 65$. A 10% margin of error was adopted in line with social science research norms where population variability is not fully known and resource constraints apply (Kothari & Garg, 2019). Stratified random sampling was then applied across three strata: academic staff ($n = 32$), administrative staff ($n = 21$), and ICT personnel ($n = 12$), ensuring proportional representation across all departments. Of the 65 questionnaires distributed, all 65 were returned and deemed usable, yielding a response rate of 100%. Readers should note that findings are specific to this institution and may not be directly generalizable to other higher learning institutions in Tanzania or beyond without further comparative study.

In addition, key informants for interviews were selected using purposive sampling. Participants such as system administrators and IT support staff were chosen based on their roles in ICT management and system administration. This technique is widely recommended in qualitative research where participants are selected based on their expertise and relevance to the research problem (Creswell & Creswell, 2018).

## Data Collection and Procedures

The data collection process was executed through a multi-stage approach designed to capture the complex relationship between technical vulnerabilities and human factors in information systems security. Primary data collection commenced with the administration of structured questionnaires to the sample population. The questionnaire was partitioned into four thematic sections: demographic profiles, information security knowledge, security attitudes, and self-reported security behaviours. This structure aligns with the widely used Knowledge-Attitude-Behaviour (KAB) model, which has been applied extensively in cybersecurity research to assess user awareness and practices (Hong et al., 2022). To ensure a high response rate and minimize bias, the researcher personally distributed the instruments across various departments and allowed respondents sufficient time to complete them. This quantitative phase was essential in establishing baseline levels of Information Systems Security Awareness (ISSA) within the institution.

Following the survey, structured interviews were conducted with key ICT personnel, including the system administrator and IT support officers. These interviews aimed to explore institutional perspectives on cybersecurity strategies, resource allocation, and the challenges associated with implementing ICT policies. Qualitative insights from these interviews provided contextual explanations for patterns observed in the survey data. Similar approaches have been used in cybersecurity studies to complement quantitative findings with organizational perspectives (Erendor & Yildirim, 2022).

In parallel with the human-centered data collection, a technical vulnerability assessment was conducted on the MWECAU's MIS using OWASP Zed Attack Proxy (ZAP). The assessment followed a standard three-stage procedure, including spidering, passive scanning, and active scanning. The spidering phase mapped the web application structure, identifying accessible pages and entry points. Passive scanning was then used to analyze system responses for potential misconfigurations. Finally, active scanning simulated real-world attacks such as SQL injection and cross-site scripting (XSS) to identify exploitable vulnerabilities. This approach is consistent with established web application security testing practices and provides empirical evidence of system weaknesses. Secondary data were collected through a documentary review of institutional ICT policies, the Cybercrimes Act of 2015, and relevant national frameworks. These documents were analyzed to assess the alignment between policy requirements and actual implementation within the institution. Previous studies have highlighted that weak policy communication and enforcement are major contributors to cybersecurity risks in higher education institutions (Hina et al., 2020).

## Reliability, Validity, and Analysis

The reliability of the research instrument was assessed using Cronbach's Alpha, with values exceeding the acceptable threshold of 0.7 for all subscales, indicating satisfactory internal consistency (Kothari & Garg, 2019). The questionnaire comprised 28 items distributed across four thematic sections: demographic profiles (5 items), information security knowledge (8 items), security attitudes (7 items), and self-reported security behaviours (8 items). Table 1 presents the Cronbach's Alpha coefficients by subscale.

**Table 1: Cronbach's Alpha Reliability Coefficients by Subscale**

| Subscale | No. of Items | Cronbach's Alpha Knowledge |
|---|---|---|
| Attitude | 8 | 0.76 |
| Behaviour | 7 | 0.81 |
| Policy & Training Awareness | 8 | 0.78 |
| Overall instrument | 5 | 0.74 |
| Total | 28 | 0.82 |

All subscale alpha values exceeded the minimum threshold of 0.70, confirming adequate internal consistency across all dimensions. Content validity was ensured through expert review by two information systems security academics who verified item relevance and clarity before pilot testing. The instrument was pilot-tested with eight staff members outside the sample, and minor item wording adjustments were made based on feedback. Quantitative data were analysed using SPSS version 27, employing descriptive statistics such as frequencies and percentages, as well as Pearson correlation analysis to examine relationships between knowledge, attitude, and behaviour.

Qualitative data obtained from interviews were analysed using thematic analysis following (Braun & Clarke's, 2006) six-phase framework: familiarization, generating initial codes, searching for themes, reviewing themes, defining and naming themes, and producing the report. Coding was conducted manually by two independent researchers, and inter-coder reliability was established through discussion of discrepancies until consensus was reached, yielding a reliability coefficient of 0.84 (Cohen's kappa). The analysis identified five major themes: (1)

limited awareness of cybersecurity threats and institutional policies; (2) inadequate formal training and capacity building; (3) positive but behaviourally inactive security attitudes; (4) weak policy communication and enforcement; and (5) technical vulnerabilities amplifying human security gaps. Representative interview quotes are presented in the Results section to support each theme. The integration of quantitative and qualitative findings enhanced the validity of the study through methodological triangulation. This approach is widely recommended in mixed-methods research to ensure consistency and reliability of results across multiple data sources (Creswell & Creswell, 2018).

## RESULTS

### Demographic Characteristics of Respondents

A total of 65 respondents participated in the study, comprising academic staff, administrative staff, and ICT personnel. All participants reported regular use of the institution's Management Information System (MIS), confirming their suitability for assessing information systems security awareness and related practices. The diversity of respondents ensured that the findings reflect a broad range of system users within the institution, capturing variations in roles, responsibilities, and levels of interaction with institutional data.

### Information Security Awareness Levels (ISSA)

The study assessed Information Systems Security Awareness across three key dimensions: knowledge, attitude, and behaviour. Overall, the findings indicate a moderate level of awareness (70%) among respondents. This suggests that while users possess a general understanding of information security concepts, significant gaps remain, particularly in translating awareness into consistent practice. Similar patterns have been reported in higher education studies, where users demonstrate reasonable awareness but fall short in applying secure behaviours consistently. To provide a clearer summary of these findings, Table 2 presents the key indicators of awareness, training, policy understanding, and behaviour.

**Table 2: Summary of Key Findings (n = 65)**

| Category | Indicator | Percentage (%) |
|---|---|---|
| Awareness | Moderate level | 70% |
| Training | No training | 66.2% |
| Policy Awareness | Not aware | 66.2% |
| Behaviour | Weak practices | ~60% |

Table 2 highlights a critical imbalance: while awareness levels are relatively moderate, both training exposure and policy awareness remain low, and actual security behaviour is weak. This imbalance provides early evidence of a disconnect between knowledge and practice.

### Conceptual Model

To contextualise the empirical findings, Figure 1 presents the conceptual model underpinning this study. The model was developed deductively from the Theory of Planned Behaviour (Ajzen, 1991) and the Knowledge–Attitude–Behaviour (KAB) framework, and was used a priori to guide data collection and instrument design. It integrates knowledge, attitude, institutional moderators (training, policy, enforcement), and system-level vulnerabilities as interacting determinants of security behaviour outcomes. The model operationalises these relationships as follows: Knowledge →Awareness →Behavioural Intention →Security Behaviour, moderated by Training and Policy Enforcement and constrained by System Vulnerabilities. The empirical findings presented below are interpreted against this framework. The model integrates the Knowledge–Attitude–Behaviour (KAB) framework with elements of the Theory of Planned Behaviour (TPB), emphasising that knowledge and attitudes influence behaviour, but are also shaped by institutional and technical factors.

CBEL Journal of Multidisciplinary Research
Vol. 1 No. 1 (2026): ISSN (Online): 3108-8848
DOI: https://doi.org/10.66313/m7r6z835
*Socio-Technical Analysis of the Awareness–Behaviour Gap in Higher Education Cybersecurity: Evidence from Tanzania*

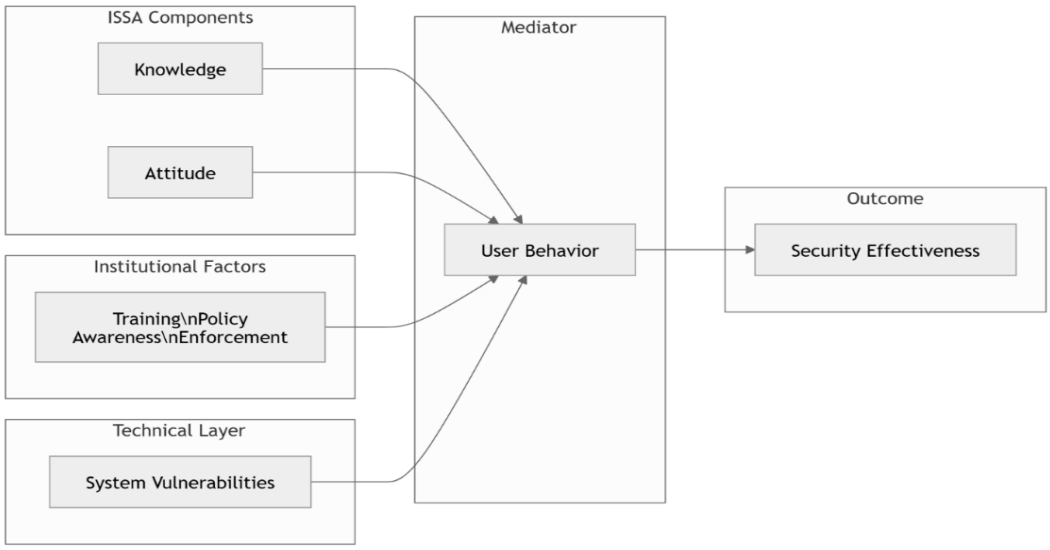


**Figure 1: Conceptual Framework of Information Systems Security**

The findings of this study strongly align with the relationships illustrated in Figure 1. The results show that knowledge and attitude contribute positively to user awareness, as evidenced by the moderate awareness level (70%; knowledge subscale: M = 3.61, SD = 0.74 on a 5-point Likert scale) and generally positive attitudinal dispositions (78.5% positive; attitude subscale: M = 3.89, SD = 0.68). These statistics confirm that knowledge and attitude contribute positively to awareness. However, the transition from awareness to actual behaviour remains weak, with approximately 60% of respondents demonstrating inconsistent or unsafe security practices.

This disconnect supports existing research such as Mobile Information Security Awareness Among Students in Higher Education: An Exploratory Study, where (Moletsane & Tsibolane, 2020) found that although users possess knowledge of security threats, this does not always result in corresponding secure behaviour. The study highlights the presence of a behavioural gap, consistent with the findings of the current research.

Furthermore, the model identifies training, policy awareness, and enforcement mechanisms as moderating factors, which influence the relationship between awareness and behaviour. This is clearly reflected in the results, where 66.2% (n = 43) of respondents reported having received no formal cybersecurity training, and 66.2% (n = 43) were unaware of any existing institutional ICT security policy. Pearson correlation analysis confirmed a significant positive relationship between training exposure and self-reported secure behaviour ($r = 0.48$, $p < 0.01$), supporting the model's positioning of training as a key behavioural moderator. Similarly, policy awareness was positively correlated with secure behavioural practices ($r = 0.41$, $p < 0.05$). A similar proportion were unaware of institutional policies. These limitations weaken the ability of users to convert knowledge into practice.

In addition, the model incorporates system vulnerabilities as a technical constraint affecting overall security effectiveness. The OWASP ZAP assessment revealed issues such as error disclosures and private IP leakage, indicating that even when users attempt to behave securely, system weaknesses may still expose the institution to risk.

The combined effect of these factors demonstrates that behaviour is not determined by awareness alone. Instead, it is shaped by a combination of individual knowledge, institutional support, and system design. This finding is consistent with studies applying the Theory of Planned Behaviour in cybersecurity, which show that behavioural outcomes depend on both internal perceptions and external enabling conditions (Erendor & Yildirim, 2022).

Overall, the conceptual model provides a useful lens for interpreting the study findings. It explains why moderate awareness does not automatically lead to secure behaviour and highlights the importance of addressing both human and technical dimensions of information systems security.

### Knowledge of Information Security

The results indicate that respondents possess basic knowledge of information security practices. Specifically, 72.3% (n = 47) correctly identified strong password requirements, and 67.7% (n = 44) could define phishing in general terms. However, deeper technical understanding remained limited: only 35.4% (n = 23) could identify common malware indicators and only 29.2% (n = 19) demonstrated knowledge of data encryption principles. Table 3 summarizes correct responses across knowledge items.

**Table 3: Knowledge of Information Security Practices (n = 65)**

| Knowledge Item | Correct Responses (n) | Percentage (%) |
|---|---|---|
| Recognition of strong password requirements | 47 | 72.3 |
| Definition of phishing | 44 | 67.7 |
| Identification of social engineering tactics | 31 | 47.7 |
| Understanding of malware indicators | 23 | 35.4 |
| Knowledge of data encryption principles | 19 | 29.2 |
| Recognition of unauthorized access signs | 26 | 40.0 |

One ICT personnel interviewee confirmed this pattern: “Most staff know they should use strong passwords, but very few understand what to do when they suspect a breach or receive a suspicious link.” A considerable proportion of respondents were therefore not familiar with advanced threats such as phishing, system vulnerabilities, or secure data handling procedures. This limitation suggests that knowledge is largely superficial and may not be sufficient to support effective decision-making in complex security situations.

### Attitude Toward Information Security

Respondents demonstrated a generally positive attitude toward information security, consistent with the weighted attitude score of 70.4% (medium level per the Kruger & Kearney, 2006 awareness scale). Table 4 presents the distribution of attitudinal scores across the three risk domains.

**Table 4: Attitude Toward Information Security by Risk Domain (n 65)**

| Domain | Attitude Score (%) |
|---|---|
| Computer Security Management | 77.3 |
| Internet & Email Management | 73.3 |
| Password Management | 63.5 |
| Overall Weighted Attitude | 70.4 |

While computer security management attracted the highest positive attitude (77.3%), password management recorded the lowest attitudinal score (63.5%), indicating that respondents were least concerned about password-related threats despite their prevalence. One respondent noted during interview: “I know I should change my password often, but we are never told why it matters or what could happen if we do not.” Many participants expressed concern about cyber threats and acknowledged the need to adopt secure practices in their daily work. This positive attitude indicates that users are not resistant to security measures, but rather may lack the necessary support or skills to implement them effectively.

### Security Behaviour

Despite moderate knowledge and positive attitudes, actual security practices were found to be inconsistent. Some respondents reported using weak passwords. The overall weighted behaviour score was 71.9% (medium level), computed using the (Kruger & Kearney, 2006) weighting formula: Overall ISSA = (Knowledge × 0.30) + (Behaviour × 0.50) + (Attitude × 0.20). Table 6 presents behaviour scores by security domain.

**Table 5: Self-Reported Security Behaviour by Domain (n = 65)**

| Security Domain | Behaviour Score (%) |
|---|---|
| Internet & Email Management | 73.3 |
| Computer Security Management | 71.8 |
| Password Management | 70.8 |
| Overall Weighted Behaviour | 71 |

While all three domains fell in the medium range (60%–79%), password management recorded the lowest 9 behavioural score. Specific risky behaviours observed included: not changing passwords periodically, sharing login credentials with colleagues, and not logging off institutional systems after use. As one respondent stated during interview: "Sometimes I leave my computer open because I will come back shortly — I did not think that was a security problem." Some respondents also, sharing login credentials, or failing to update their credentials regularly. These behaviours expose the system to potential risks and demonstrate that awareness does not automatically translate into secure action.

This pattern reflects what has been described in the literature as a knowledge–practice gap, where users understand security concepts but fail to apply them consistently in real-world situations. The findings therefore confirm the existence of an awareness–behaviour gap within the institution.

### Training and Policy Awareness

The study further examined institutional support mechanisms, focusing on training and policy communication. The findings reveal that 66.2% (n = 43) of respondents had not received any formal training in information security. In addition, only 33.8% (n = 22) of respondents were aware of existing ICT security policies within the institution. Table 6 presents the detailed breakdown of responses on training and policy awareness items.

**Table 6: Training and Policy Awareness Responses (n = 65; values as % Agree/Strongly Agree)**

| Statement | Strongly Disagree (%) | Disagree (%) | Do Not Know (%) | Agree (%) | Strongly Agree (%) |
|---|---|---|---|---|---|
| I know the institution has an ICT security policy | 5.8 | 13.5 | 25.0 | 42.3 | 13.5 |
| ICT policy is conveyed to all employees | 19.2 | 28.8 | 26.9 | 23.1 | 1.9 |
| I have read the institution's ICT security policy | 32.7 | 26.9 | 23.1 | 13.5 | 3.8 |
| ICT policy is periodically reviewed | 17.3 | 11.5 | 55.8 | 7.7 | 7.7 |
| I have received information security awareness training | 30.8 | 40.4 | 11.5 | 11.5 | 3.8 |
| I have been informed on what to do in case of a security threat | 21.2 | 34.6 | 7.7 | 23.1 | 13.5 |
| I would attend institutional IT security training | 7.7 | 13.5 | 7.7 | 30.8 | 40.4 |

Notably, while 71.2% of respondents had not received formal information security training, 71.2% expressed willingness to attend such training if offered. This suggests that the barrier to improved security behaviour is institutional, not attitudinal. A key informant from the ICT Directorate confirmed: "The ICT policy was developed but by then we had few IT resources and few computers; we are now working on a new one and planning to involve employees when the first draft is out to have their inputs."

These results suggest that institutional efforts to promote secure practices are limited. The absence of structured training reduces users' ability to apply security knowledge effectively, while low policy awareness indicates weak communication and enforcement mechanisms. Previous studies have shown that lack of training and policy awareness significantly contributes to poor cybersecurity practices in higher education environments.

### System Vulnerability Assessment

The technical assessment of the institution's MIS, conducted using OWASP ZAP version 2.12.0 (unauthenticated scan, authorized by the ICT Directorate), revealed six distinct vulnerability types. The ZAP Summary Report classified these as: High risk = 0, Medium risk = 2, Low risk = 4, Informational = 0. Table 7 presents the full findings.

**Table 7: OWASP ZAP Vulnerability Assessment Results**

| Vulnerability | Risk Level | Instances | Security Implication |
|---|---|---|---|
| Application Error Disclosure | Medium | 14 | Server error messages expose stack traces and file paths, enabling targeted reconnaissance by attackers X-Frame-Options |
| Header Not Set | Medium | 49 | Absence of X-Frame-Options header exposes pages to clickjacking (UI redressing) attacks |
| Cross-Domain JavaScript Source File Inclusion | Low | 24 | Pages include third-party scripts outside institutional control, risking unexpected or malicious functionality |
| Private IP Address Disclosure | Low | 5 | Internal IP addresses leaked in HTTP response body, potentially exposing internal network |
| Web Browser XSS Protection Not Enabled | Low | 199 | X-XSS-Protection header not configured, leaving users exposed to reflected cross-site scripting attacks |
| X-Content-Type-Options Header Missing | Low | 98 | Browser forced to guess MIME content type, increasing risk of MIME-sniffing-based attacks |

Remediation recommendations include: (1) implementing custom error pages to suppress verbose error messages and stack traces; (2) setting the X-Frame-Options header to SAMEORIGIN or DENY on all responses; (3) auditing and removing unnecessary cross-domain script inclusions; (4) stripping internal IP headers at the reverse proxy; (5) adding X-XSS-Protection: 1; mode=block to all HTTP responses; and (6) setting X-Content-Type-Options: nosniff globally. All identified vulnerabilities are configurable at the web server or application layer and do not require code changes, indicating that basic secure configuration management practices are absent from the institution's development and deployment workflow.

These findings demonstrate that security challenges are not limited to user behaviour but also exist at the system level. The presence of such vulnerabilities increases the likelihood that human errors or unsafe practices could lead to successful cyberattacks. In addition to the identified system vulnerabilities, the study observed that some users were operating computers with non-genuine or cracked versions of the Windows operating system. This practice introduces significant cybersecurity risks because unauthorized operating systems often lack official security updates, patches, and vendor support. As a result, such systems become more vulnerable to malware infections, unauthorized access, and exploitation by attackers. Previous studies have shown that pirated software can expose users to malicious code, spyware, and system backdoors, thereby increasing institutional cybersecurity risks (Iqbal et al., 2024).

### Integration of Human and Technical Findings

When the human and technical findings are considered together, a clear pattern emerges. On one hand, users demonstrate moderate awareness but inconsistent security behaviour. On the other hand, the system itself contains identifiable vulnerabilities. This combination significantly increases the overall security risk. For instance, a user who lacks strong security practices may unintentionally exploit system weaknesses, creating entry points for attackers. This interaction between human behaviour and technical flaws highlights the need for a comprehensive approach to cybersecurity that addresses both dimensions simultaneously.

As illustrated in Figure 1, user behaviour is influenced by knowledge and attitude but is also shaped by institutional factors such as training and policy enforcement, while system vulnerabilities further constrain security outcomes. The findings of this study align closely with this framework, confirming that both human and technical factors jointly determine the effectiveness of information systems security.

### The Awareness–Behaviour Gap

The most significant finding of this study is the existence of a clear awareness–behaviour gap. While users demonstrate moderate awareness and positive attitudes toward information security, this does not consistently translate into secure practices. This gap appears to be influenced by several interconnected factors, including limited access to formal training, low awareness of institutional policies, weak enforcement mechanisms, and the presence of technical system vulnerabilities. These factors collectively limit users' ability to act securely, even when they understand the importance of information security. The findings reinforce the argument that improving awareness alone is insufficient. Without adequate institutional support and robust technical safeguards, users are unlikely to consistently adopt secure behaviours. This insight is consistent with emerging research in higher education, which emphasizes the need for integrated, human-centered cybersecurity strategies.

## DISCUSSION

### Knowledge and Awareness in Information Systems Security

The findings indicate that respondents possess a moderate level of information systems security awareness, with basic knowledge of common practices such as password protection and safe internet usage. However, this knowledge remains largely superficial, particularly in relation to advanced threats such as phishing and system vulnerabilities. Within the conceptual model (Figure 1), knowledge represents a foundational component influencing user behaviour.

The results suggest that while knowledge contributes positively to awareness, it is not sufficiently deep to support consistent secure practices. This observation aligns with findings from Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees by Al-Shanfari et al. (2022), which shows that awareness alone does not guarantee secure behaviour unless supported by practical understanding and enabling conditions.

In the context of this study, knowledge appears to function more as a theoretical awareness rather than actionable competence. This limits its direct influence on behaviour, reinforcing the idea that knowledge must be complemented by other factors to produce meaningful security outcomes.

### Attitude and Perception Toward Information Security

The study reveals that respondents generally hold positive attitudes toward information security, recognizing its importance in protecting institutional data. Within the conceptual framework, attitude is expected to influence behavioural intention. However, the findings demonstrate that positive attitudes alone do not translate into secure behaviour. This disconnect is consistent with the Theory of Planned Behaviour, which argues that

attitudes must be supported by perceived behavioural control and external conditions to influence actual behaviour. Evidence from Digital Workplaces and Information Security Behaviour of Business Employees: An Empirical Study of Saudi Arabia by Saeed (2023) shows that even when employees recognize the importance of cybersecurity, they may still fail to adopt secure practices due to lack of institutional support and practical constraints. In this study, the positive attitudes observed among respondents indicate readiness for secure behaviour, but this readiness is not fully realized due to gaps in training, policy awareness, and system support.

## Security Behaviour and the Awareness–Behaviour Gap

The most critical finding of this study is the inconsistency between awareness and actual behaviour. Despite moderate knowledge and positive attitudes, a significant proportion of respondents engage in unsafe practices such as weak password usage and credential sharing. Within the conceptual model, behaviour acts as the central link between awareness and security outcomes. The observed inconsistency confirms the existence of an awareness–behaviour gap, where users understand security concepts but fail to apply them consistently.

This finding is supported by Exploring the Cybersecurity-Resilience Gap: An Analysis of Student Attitudes and Behaviours in Higher Education by Goliath et al. (2024), which identifies a similar gap between cybersecurity awareness and actual practices in higher education settings. The study emphasizes that awareness alone is insufficient and that behavioural change requires targeted interventions. The persistence of unsafe practices in this study indicates that behavioural outcomes are influenced by more than awareness, reinforcing the need to consider moderating and contextual factors.

## Role of Training, Policy Awareness, and Institutional Support

The conceptual model identifies training, policy awareness, and enforcement mechanisms as key moderating factors influencing behaviour. The findings strongly support this relationship. A majority of respondents reported lack of formal training, and a significant proportion were unaware of institutional security policies. These gaps weaken the link between awareness and behaviour by limiting users' ability to translate knowledge into action. Training enhances practical skills, while policy awareness establishes expected standards of behaviour. Without these elements, users operate without clear guidance or accountability.

Empirical support is found in Cybersecurity Awareness, and Cybersecurity Behaviour of High School Students in Davao City: A Mediation Role of Perceived Behavioural Control by Booc et al. (2024), which shows that perceived control, often shaped by training and institutional support, significantly influences cybersecurity behaviour. In this study, the absence of structured training and weak policy communication reduce users' perceived ability to act securely, thereby weakening behavioural outcomes.

## Influence of System Vulnerabilities on Security Outcomes

Beyond human factors, the conceptual model incorporates system vulnerabilities as a technical constraint affecting security effectiveness. The findings from the OWASP ZAP assessment confirm the presence of vulnerabilities such as error disclosures and IP leakage. These weaknesses indicate that even if users adopt secure behaviours, the system itself may still be exposed to risks. This highlights the importance of viewing cybersecurity as a socio-technical issue, where human behaviour and system design interact.

The presence of vulnerabilities amplifies the consequences of poor user behaviour. For example, weak password practices combined with system misconfigurations can significantly increase the likelihood of unauthorized access. This interaction reinforces the need for integrated security strategies that address both human and technical dimensions.

The discovery of cracked or non-genuine operating systems among some users further increases institutional security risks. Pirated operating systems typically do not receive official security updates and may contain hidden malware or unauthorized modifications. This creates additional vulnerabilities that can compromise both user devices and institutional networks. The finding supports the argument that cybersecurity challenges in higher learning institutions are not limited to user awareness alone, but also involve software legitimacy and infrastructure management. Similar concerns have been raised in cybersecurity literature, where pirated software has been associated with malware distribution and weakened system protection (Iqbal et al., 2024).

### Integrated Interpretation of the Conceptual Model

When all elements of the conceptual model are considered together, the findings provide a coherent explanation of the awareness–behaviour gap observed in this study. Knowledge and attitude contribute to awareness, but their influence on behaviour is moderated by training, policy awareness, and institutional support. At the same time, system vulnerabilities impose additional constraints on security effectiveness.

This integrated perspective aligns with extensions of the Theory of Planned Behaviour, such as those discussed in The Theory of Planned Behaviour and Information Security Policy Compliance by Sommestad et al. (2019), which argue that additional contextual factors are necessary to fully explain security behaviour. In the context of this study, the awareness–behaviour gap emerges as a result of multiple interacting factors rather than a single deficiency. Addressing this gap therefore requires a comprehensive approach that strengthens knowledge, enhances training, improves policy communication, and secures system infrastructure. Furthermore, the technical vulnerabilities found, specifically the application error disclosures, point to a lack of Hardening Standards in the Software Development Life Cycle (SDLC). In contemporary cybersecurity (2020–2025), "Security by Design" is no longer optional. The presence of these flaws indicates that ICT administrators are not performing routine automated audits, a failure that persists across many Tanzanian HLIs due to human resource constraints (Chacha et al., 2024).

## CONCLUSION

This study examined the relationship between information systems security awareness and user behaviour within a higher learning institution in Tanzania. The findings reveal that although users demonstrate moderate awareness and positive attitudes toward information security, this does not consistently translate into secure practices. This confirms the existence of an awareness–behaviour gap, where knowledge alone is insufficient to influence behaviour.

The study further shows that this gap is influenced by multiple factors, including lack of formal training, low awareness of institutional policies, weak enforcement mechanisms, and the presence of technical system vulnerabilities. These factors interact to create an environment where users are unable to consistently adopt secure practices, even when they understand their importance.

By integrating both human and technical perspectives, this study contributes to the understanding of cybersecurity challenges in higher learning institutions, particularly in developing contexts. It highlights the need to move beyond awareness-focused approaches toward more comprehensive strategies that address both behavioural and system-level risks.

## RECOMMENDATIONS

Based on the findings of this study, several recommendations are proposed to improve information systems security in higher learning institutions.

i. First, institutions should implement continuous and practical cybersecurity training programs. Training should focus not only on awareness but also on real-life application, enabling users to develop the skills needed to respond to security threats effectively.
ii. Second, there is a need to strengthen policy communication and enforcement. ICT security policies should be clearly communicated, regularly updated, and actively enforced. Users should be made aware of their responsibilities and the consequences of non-compliance.
iii. Third, institutions should adopt a holistic cybersecurity approach that integrates human and technical measures. This includes combining user education with strong system controls such as access management, monitoring, and regular updates.
iv. Fourth, regular vulnerability assessments should be conducted to identify and address system weaknesses. Tools such as OWASP ZAP can be used periodically to ensure that systems remain secure against emerging threats.
v. Fifth, institutions should promote a security-aware culture, where information security is viewed as a shared responsibility. This can be achieved through awareness campaigns, leadership support, and encouraging responsible user behaviour.
vi. Finally, future research should expand the scope of this study by including multiple institutions and applying advanced statistical techniques to further explore the relationships between awareness, behaviour, and security outcomes.

## DECLARATIONS

### Conflict of Interest

The authors declare that they have no competing interests.

### Ethical Approval

The study was conducted in accordance with the ethical principles governing research involving human participants. Ethical approval was obtained from the Mwenge Catholic University ethics committee prior to the commencement of fieldwork. Administrative permission to conduct the study was obtained from the Kilimanjaro Regional Commissioner's Office.

### Informed Consent

Informed consent was obtained from all individual participants included in the study before data collection commenced. Participation was voluntary, and respondents were informed of their right to withdraw from the study at any stage without any adverse consequences.

**Data Availability:** Anonymised data are available from the corresponding author upon reasonable request.

### Consent for Publication

The Authors have accepted the article to be published in the CBEL Journal of Multidisciplinary Research.

## REFERENCES

Ajzen, I. (1991). The theory of planned behaviour. *Organizational Behaviour and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Alam, S., Ahsan, N., Kokash, H., Alam, S., & Ahmed, S. (2024). Students' behaviours in information security: Extension of protection motivation theory. *Information Security Journal: A Global Perspective, 34*, 191–213.

Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. *Big Data and Cognitive Computing*.

Al-Shanfari, I., Yassin, W., Tabook, N., Ismail, R., & Ismail, A. (2022). Determinants of information security awareness and behaviour strategies in public sector organizations among employees. International Journal of Advanced Computer Science and Applications, 13(10), 742–751.

Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods. *IEEE*.

Amoresano, K., & Yankson, B. (2023). Human error: A critical contributing factor to the rise in data breaches: A case study of higher education. *HOLISTICA – Journal of Business and Public Administration, 14*, 110–132.

Booc, N. B. B., Budiongan, K., & Carballo, R. C. (2024). Cybersecurity awareness and cybersecurity behaviour of high school students in Davao City: A mediation role of perceived behavioural control. European Journal of Applied Science, Engineering and Technology.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Chacha, M., Mvungi, N. H., & Sinde, R. (2024). Cyber security maturity assessment framework for higher learning institutions in developing countries. International Journal of Computing and ICT Research, 17(1), 45-62.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications

Erendor, M. E., & Yildirim, M. (2022). Cybersecurity awareness in online education: A case study analysis. *IEEE*.

Goliath, S., Tsibolane, P., & Snyman, D. (2024). Exploring the cybersecurity-resilience gap: An analysis of student attitudes and behaviours in higher education. arXiv. https://arxiv.org/abs/2411.03219

Hina, S., Dhanapal, P., & Dominic, D. (2020). Information security policies' compliance: A perspective for higher education institutions. *Journal of Computer Information Systems*.

Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V., & Xu, X. (2022). The influence of social education level on cybersecurity awareness and behaviour. *Education and Information Technologies*.

Iqbal, A., Aman, M., Rejendran, R., & Sikdar, B. (2024). Unveiling the connection between malware and pirated software in Southeast Asian countries: A case study. IEEE Open Journal of the Computer Society, 5, 62–72.

Kothari, C. R., & Garg, G. (2019). Research methodology: Method & techniques (Fourth edition.). New Delhi: New Age International Publishers.

Moletsane, T., & Tsibolane, P. (2020). Mobile information security awareness among students in higher education: An exploratory study. In 2020 Conference on Information Communications Technology and Society (ICTAS) (pp. 1–6). IEEE. https://doi.org/10.1109/ICTAS47918.2020.233972

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cybersecurity within healthcare organisations: A systematic review. *Sensors, 21*(15), 5119. https://doi.org/10.3390/s21155119

Parikh, V., & Nimbekar, M. (2023). Socializing the impact: An analysis of the theory of planned behaviour's influence on increasing university students' cybersecurity awareness. *Journal of Community Development*.

Saeed, S. (2023). Digital workplaces and information security behaviour of business employees: An empirical study of Saudi Arabia. Sustainability, 15(3), 1–18. https://doi.org/10.3390/su15032345

Sife, A. S. (2022). Cyber security awareness among undergraduate students in Tanzania: A case of Sokoine University of Agriculture. University of Dar es Salaam Library Journal, 17(2), 34-51.

Sommestad, T., Karlzén, H., & Hallberg, J. (2019). The theory of planned behaviour and information security policy compliance. Journal of Computer Information Systems, 59(4), 344–353. https://doi.org/10.1080/08874417.2017.1368421

Temu, D. J. (2017). Information systems security in higher learning institutions: The case of one university in Tanzania [Master's dissertation, Institute of Accountancy Arusha]. IAA Institutional Repository. https://repository.iaa.ac.tz/

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy, 2*(3), 573–586. https://doi.org/10.3390/jcp2030029

United Republic of Tanzania. (2015). The Cybercrimes Act, 2015. Government Printer.

Zwilling, M., Klein, G., Lesjak, D., Wiechetek, Ł., Çetin, F., & Basım, H. N. (2020). Cyber security awareness, knowledge and behaviour: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97. https://doi.org/10.1080/08874417.2019.1650678

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.05.001