East African Journal of Education and Social Sciences
EAJESS July-August 2025, Vol. 6, No. 4, pp. 79-87.
ISSN: 2714-2132 (Online), 2714-2183 (Print). Published by G-Card
DOI: https://doi.org/10.46606/eajess2025v06i04.0457.

Behavioral, Organizational and Cultural Determinants of ICT Security Incident Reporting in Tanzanian Public Higher Learning Institutions

Adam Aloyce Semlambo
ORCiD: https://orcid.org/0000-0002-6839-0215
Department of Computer Science, Institute of Accountancy Arusha, Tanzania
Email: semlambo@gmail.com

Abstract

In the face of escalating cyber threats, Tanzanian public higher learning institutions (PHLIs) face unique challenges in ICT security incident reporting due to organizational, behavioral and cultural barriers. While previous studies emphasized the role of socio-technical factors in shaping cybersecurity practices, there is a distinct research gap regarding how these factors manifest in resource-constrained African academic environments. This study aimed to investigate the behavioral, organizational and cultural factors influencing incident reporting behavior in Tanzanian PHLIs. Employing a sequential explanatory mixed-methods design, the study surveyed 384 participants and conducted interviews with 30 key informants across eight purposively selected institutions, using stratified and systematic random sampling techniques. Key findings revealed that while staff recognize reporting as their responsibility and understand required procedures, fear of blame, lack of trust in confidentiality, inadequate training and weak leadership engagement significantly hinder actual reporting practices. Statistical analysis confirmed that organizational enablers, such as leadership support, regular training and clear confidential reporting mechanisms significantly correlated with improved reporting behavior, whereas demographic variables had no significant impact. These findings underscore the importance of aligning technical systems with institutional culture and user behavior. The study recommends decentralizing reporting channels, implementing anonymous mechanisms, reinforcing leadership support and reviewing ICT policies to foster a proactive and resilient cybersecurity environment in Tanzanian PHLIs.

Keywords: ICT Security; incident reporting' public higher learning institutions; organizational behavior; socio-technical systems theory.

How to cite: Semlambo, A. A. (2025). Behavioral, Organizational and Cultural Determinants of ICT Security Incident Reporting in Tanzanian Public Higher Learning Institutions. East African Journal of Education and Social Sciences 6(4), 79-87. DOI: https://doi.org/10.46606/eajess2025v06i04.0457.

Introduction

The rise of cyber threats has shifted attention toward the preparedness and resilience of institutions handling sensitive information (ENISA, 2020), including public higher learning institutions (PHLIs). These institutions are custodians of extensive personal and research data, making them attractive targets for cybercriminals (Verizon, 2021).

Incident reporting is a critical component of any institutional cybersecurity strategy. However, reporting behavior is deeply influenced by individual, organizational and cultural factors, including trust, perceived risk, fear of blame and policy awareness (Alshaikh et al., 2021; Choi et al., 2023). Studies indicate that users are more likely to report incidents in environments with supportive leadership, clear policies and confidential reporting mechanisms (Adams & Sasse, 2019; Pahnila et al., 2015). In Tanzanian PHLIs, Semlambo's (2025) study, only three out of eight public higher learning institutions had a defined audit cycle and none reviewed their ICT security policy more frequently than every two years, highlighting a systemic absence of dedicated reporting procedures that foster normalization of non-reporting and circumvention of formal channels. Additionally, employees often do not perceive reporting as their responsibility, especially when fear of blame and sanctions is a potential outcome (Rezgui & Marks, 2015; Bada et al., 2019).

Scholarly work has long emphasized the importance of a socio-technical approach, which considers the interdependent relationship between human (social) and technological (technical) elements within organizations in addressing cybersecurity behaviors (Zoto et al., 2018; Gundu & Flowerday, 2020). This perspective recognizes that technical solutions alone are insufficient unless aligned with user behavior, institutional culture and communication practices. Yet, much of the existing research on cybersecurity incident reporting is concentrated in developed contexts, where studies, such as those by Adams and Sasse (2019) and Choi et al. (2023) highlight the importance of leadership support, confidentiality and user trust. These findings emerge from institutional environments with mature IT infrastructures and high awareness levels, conditions that differ significantly from those in African academic institutions. As such, these studies leave a gap in understanding how similar socio-technical factors operate in resource-constrained environments like Tanzania, where issues, such as hierarchical structures, limited training budgets and understaffed IT departments, uniquely shape breach disclosure behavior (Semlambo, 2025).

In Tanzania, cybersecurity is managed through frameworks guided by the e-Government Authority (eGA), yet compliance and cyber security enforcement mechanisms remain limited and highly centralized (Semlambo, 2025). While policies exist, they are often embedded within broader ICT frameworks and lack the clarity and specificity required to promote incident reporting behavior among academic staff, IT personnel and administrative units (Alqahtani & Kavakli, 2022). Cyber incidents are often underreported, and when reported, they are inconsistently recorded, creating a reactive rather than proactive security culture (Park & Kim, 2020).

Despite a steady increase in cyber threats targeting Tanzania's higher education sector, empirical research on the behavioral, cultural and organizational factors influencing security incident reporting in PHLIs remains limited. In 2023 alone, the Tanzania Computer Emergency Response Team (TZ-CERT) recorded over 16,000 attempted cyberattacks targeting key sectors, including education, underscoring the urgency of addressing cybersecurity behaviors at the institutional level (Tanzania Computer Emergency Response Team, 2023). National ICT policies do not adequately address the institutional realities or support structures necessary to foster consistent breach disclosure. This policy-practice gap leads to poor risk visibility, lack of incident trend data and minimal institutional learning. Therefore, understanding what enables or hinders incident reporting in Tanzanian academic institutions is crucial for improving cybersecurity resilience and developing user-aligned response frameworks. In response, this study examined the behavioral, organizational and cultural factors that affect security incident reporting behavior in Tanzania's public higher education institutions.

Literature Review

Cybersecurity incident reporting is shaped not only by technological infrastructure but also by complex behavioral and organizational dynamics. This section reviews both theoretical foundations and empirical findings to contextualize the socio-technical factors influencing reporting behavior, particularly within public higher learning institutions (PHLIs) in sub-Saharan Africa.

Theoretical Underpinnings

This study is grounded in the Socio-Technical Systems (STS) Theory, which emphasizes the interdependence between people (social systems) and technologies (technical systems) within organizations. Originally developed by Trist and Emery in the 1950s, STS has evolved into a foundational theory for analyzing how humans interact with technological infrastructures in complex environments, such as universities (Zoto et al., 2018). In the context of Tanzanian PHLIs, this theory offers a suitable lens for examining how organizational structure, leadership, reporting policies, training programs and user behavior influence incident reporting outcomes (Semlambo, 2025). As Semlambo

(2025) highlights, the lack of integration between technical controls (e.g., firewalls, monitoring systems) and social enablers (e.g., trust, confidentiality, training, awareness) results in low policy compliance and a culture of silence surrounding breach reporting.

STS theory suggests that effective information security management cannot rely solely on technical safeguards but must also align with human values, routines, and communication flows. In PHLI settings, where IT departments are understaffed and policies are often generalized, applying the socio-technical approach can reveal why reporting behaviors vary across institutions. This aligns with previous work by Zoto et al. (2018), who found that incorporating systems thinking into cybersecurity education and policy design led to greater reporting clarity and behavioral change. Therefore, the STS framework not only explains the behavior of individuals within security ecosystems but also informs how policy, structure and user engagement can be co-designed to enhance incident response.

Empirical Literature Review

Empirical studies on information security reporting behavior have emphasized that human behavior is the weakest link in cybersecurity management. Employees often fail to report security incidents due to fear of blame, unclear procedures or lack of awareness (Bada et al., 2019). In a study involving university staff in Malaysia, Masrek and Mohd Sam (2017) found that only 37% of users were aware of any formal incident reporting policy and even fewer understood how to report an incident when one occurred. Similar patterns emerge in Tanzanian PHLIs, where Semlambo (2025) found that in 5 out of 8 universities studied, no standalone reporting policy existed and the majority of staff reported breaches informally or not at all. These findings support the argument that without clear and user-centered policies, reporting behavior is likely to remain inconsistent and ineffective.

Another theme emerging from the literature is the role of perceived risk and trust in influencing reporting behavior. Users are more likely to report incidents when they trust that the process is confidential and that no punitive measures will be taken (Choi et al., 2023; Park & Kim, 2020). Semlambo (2025) found that junior staff were less likely to report due to fear of victimization or being blamed for the breach. The lack of leadership communication on the value of reporting further discouraged disclosure. These insights align with findings by Alshaikh et al. (2021), who noted that strong leadership and organizational support foster a culture of openness in breach disclosure practices. The presence of clearly communicated policies and support structures positively correlated with willingness to report incidents.

Organizational structure and cultural factors have been empirically shown to influence incident reporting behavior. For example, Masrek and Mohd Sam (2017) found that in a Malaysian university, only 37% of staff were aware of a formal incident reporting policy and even fewer engaged with reporting procedures pointing to policy centralization and ambiguity as barriers. Similarly, Bada et al. (2019) observed that in rigid institutional cultures, fear of sanctions and unclear reporting responsibilities significantly reduced disclosure rates. The study also revealed that only three institutions had regular security awareness programs, and those that did demonstrated notably higher levels of incident reporting. This supports findings by Masrek and Mohd Sam (2017) and Pahnila et al. (2015), who reported that training, feedback mechanisms and participatory policy design all enhance reporting behavior. Moreover, Bada et al. (2019) argued that awareness campaigns must be paired with structural reforms, such as anonymous reporting and decentralized reporting offices to yield sustainable results.

Despite these contributions, significant gaps remain in understanding the interplay of behavioral, organizational and cultural factors in incident reporting, especially in the context of African higher educational institutions. Most existing studies are either conceptual or were conducted in Western or Asian settings, with limited empirical research in sub-Saharan African PHLIs (Zoto et al., 2018; Alqahtani & Kavakli, 2022). In Tanzania, national ICT frameworks lack implementation guidelines, tailored to academic institutions. Semlambo's (2025) findings highlight this disconnect, as institutional behavior often contradicts national cybersecurity intentions. Therefore, there is a pressing need for context-specific studies that explore how reporting behavior is shaped by institutional culture, leadership style and staff perceptions within African universities. This study seeks to fill that gap.

Methodology

This study employed a mixed-methods research approach, grounded in pragmatism, to investigate the behavioral, organizational and cultural factors influencing incident reporting in Tanzanian public higher education institutions. The social constructivist ontological stance guided the exploration of diverse stakeholder perspectives on ICT security, recognizing the socially constructed nature of institutional policies and behaviors. According to Semlambo (2025), institutional cybersecurity policies in Tanzanian PHLIs are socially embedded and often reflect local organizational norms, which shape how reporting practices are understood and enacted across different institutional levels. The pragmatic epistemology enabled the integration of qualitative insights with empirical data to produce actionable recommendations for institutions (Creswell, 2009; Bryman, 2016). The study adopted the sequential explanatory mixed-methods design.

Population and Sampling

The study population included ICT officers, academic staff and administrative staff from eight public higher learning institutions (PHLIs) in Tanzania. These eight institutions were purposely selected from a total of 32 public PHLIs, based on criteria, such as institutional size, geographic distribution and maturity of ICT infrastructure, to ensure diversity and contextual relevance. The total population across these institutions was 2,727, where a sample of 384 was drawn, including staff members. Stratified sampling was used to group participants by role ICT officers, academic staff, and administrative staff. Within each stratum, systematic random sampling was employed to ensure representativeness. For the qualitative phase, 30 participants were selected through purposive sampling, based on their practical experience with ICT policy implementation and incident reporting (Creswell, 2009).

Data Collection Procedures

Data collection employed a sequential explanatory approach. In the first phase, a 5-point Likert scale structured questionnaire distributed to 384 respondents across the selected institutions to gather quantifiable data on incident reporting behavior, policy awareness and institutional practices. In the second phase, semi-structured interviews were conducted with 30 participants to explore underlying beliefs, motivations and institutional norms that influence reporting behavior. As Semlambo (2025) observed, staff reporting behavior is often shaped by institutional cultures of fear and informal norms, where breaches are resolved quietly rather than reported through official channels. This combination of tools allowed the researcher to measure trends and explore contextual nuances, aligning with the pragmatist goal of balancing objectivity with meaning-making.

Data Analysis

Quantitative data from the questionnaire was analyzed using the SPSS, employing both descriptive and inferential statistics to assess trends and relationships among variables. Chi-square test was selected as an appropriate statistical tool for examining relationships. Although Chi-square is a non-parametric test and generally less powerful than parametric alternatives, it is particularly suited for analyzing nominal data and assessing correlations between variables. Qualitative data was analyzed using the thematic approach, following a six-step coding framework to identify patterns, insights and institutional narratives. According to Braun and Clarke (2006), thematic analysis involves identifying, analyzing and reporting patterns (themes) within data, offering a flexible and accessible approach to interpreting qualitative information. Triangulation was employed to merge insights from both datasets, ensuring that the statistical findings were supported and contextualized by lived experience.

Validity and Reliability

To ensure the quality of the research instruments, both face and content validity were established through expert review by ICT policy and cybersecurity scholars. A pilot test was conducted to refine the questionnaire items for clarity and relevance. For internal consistency, Cronbach's alpha was computed, with values above the 0.70 threshold indicating acceptable reliability for the constructs measured. In the qualitative phase, credibility was ensured through member checking, where selected participants reviewed and validated their interview transcripts. Triangulation of quantitative and qualitative data further enhanced the study's overall trustworthiness, allowing for cross-validation of findings (Creswell, 2009).

Ethical Considerations

This study adhered to established ethical standards for research, involving human participants. Ethical clearance was obtained from the relevant university ethics committee prior to data collection. Informed consent was secured from all participants, who were assured of their right to withdraw at any stage without penalty. Anonymity and confidentiality were strictly maintained by de-identifying responses and storing data securely. Additionally, care was taken to ensure that no participant faced risk of reprisal for disclosing information related to ICT incidents or institutional policies. The study prioritized voluntary participation, data protection, and transparency throughout the research process (Creswell, 2009).

Findings and Discussion

This section presents the findings along with discussions based on literature.

Research Question 1: What are the perceived behavioral, organizational and cultural factors that that influence staff agreement with ICT security incident reporting practices?

The first item in Table 1 determines whether staff perceived incident reporting as part of their professional responsibility while the second assessed their awareness of reporting procedures.

Table 1: Respondents' Agreement with Incident Reporting Indicators

#	Statement in the Questionnaire	Mean	SD	Interpretation
1	Reporting incidents is part of my responsibility	4.12	0.76	Agree
2	I know the procedures for reporting ICT security incidents	3.88	0.81	Agree
3	Reporting channels in my institution are clearly defined	3.26	1.12	Neutral
4	I trust that my report will be kept confidential	2.98	1.05	Neutral
5	I fear I may be blamed or punished if I report an incident	3.47	0.97	Agree (negatively framed)
6	ICT policies in my institution are easy to understand	3.15	0.90	Neutral
7	Training on reporting procedures is provided regularly	2.85	0.88	Disagree
8	There is sufficient support from ICT leadership	3.04	0.95	Neutral
9	There is a culture that encourages reporting	3.22	1.03	Neutral
10	I reported an ICT security incident in the past 12 months	2.61	1.17	Disagree

Findings show high agreement on both counts Mean = 4.12 and 3.88, respectively indicating that staff generally understood their role in incident reporting and were familiar with institutional procedures. However, these findings alone do not confirm whether this awareness consistently translates into actual reporting behavior. From the lens of the Socio-Technical Systems (STS) Theory, this suggests that while the social subsystem—comprising knowledge and perceived responsibility is present, it may not be adequately integrated with technical and organizational supports (Zoto et al., 2018; Semlambo, 2025).

According to Adams and Sasse (2019), users are more likely to comply with security policies in environments where leadership support and confidential mechanisms reinforce individual awareness and responsibility. One participant expressed a challenge, "We are told it's our responsibility, and I know what to do but the environment doesn't always make it easy to report." Such sentiments highlight that while procedural knowledge exists, supportive organizational conditions are critical to turning awareness into consistent reporting behavior.

The third item in Table 1 focused on the clarity of institutional reporting mechanisms. Respondents gave a neutral rating (Mean = 3.26), indicating uncertainty in how clearly these channels are defined across institutions. Additional items, such as perceptions of leadership support (Item 8, Mean = 3.04) and the existence of a reporting-supportive culture (Item 9, Mean = 3.22), received neutral responses. These findings suggest organizational ambiguity and limited proactive engagement from leadership in fostering a reporting environment. From an STS Theory perspective, the technical systems, such as reporting protocols appear underdeveloped or disconnected from the social structures that drive reporting behavior (Zoto et al., 2018). This echoes Bada et al. (2019), who observed that unclear procedures and weak institutional cultures discourage reporting. One interviewee captured this hesitation aptly: “There’s no clear channel. Even if something happens, we just fix it ourselves quietly.” This indicates that the lack of well-communicated, trusted reporting mechanisms not only confuses users but also encourages informal and untraceable incident responses.

The fifth item in Table 1 measured whether staff fear being blamed or punished for reporting an incident, with a mean score of 3.47. This value indicates a leaning toward agreement, though not strongly, suggesting that fear of reprisal may be present among some staff but not uniformly felt. This supports the view that psychological safety is a concern, albeit not an overwhelming one. From the Socio-Technical Systems perspective, such fear points to a misalignment between the social components trust, communication and institutional norms and the technical expectations of formal reporting (Semlambo, 2025). As Choi et al. (2023) argue, environments perceived as punitive discourage disclosure. A participant illustrated this tension, saying, “If you report, you’re the one who gets questioned, as if it’s your fault.” This reflects a broader cultural issue, where the act of reporting can be misinterpreted as an admission of guilt, undermining staff confidence in institutional processes and deterring engagement with formal reporting channels.

To address these challenges, institutions must decentralize reporting channels, provide clear and confidential procedures, and institutionalize regular training. Leadership must actively foster a culture of openness and review ICT policies every four years as recommended by the study. Applying a socio-technical lens, institutions should realign technical systems with staff realities, ensuring that policy, leadership, and culture co-evolve to improve security incident reporting practices.

Inferential Statistics Analysis

To determine whether relationships exist between staff characteristics and incident reporting behavior, the Chi-square test of independence was employed. This non-parametric test is appropriate for identifying associations between categorical variables.

Research Question 2: Is there a significant relationship between staff demographic variables, such as role and incident reporting behavior?

Chi-Square Test: Staff Role and Reporting Behavior

Table 2 presents the Chi-square test results assessing the relationship between staff role (ICT officers, academic staff, and administrative staff) and incident reporting behavior. The analysis yielded a Chi-square value of 9.55 with 8 degrees of freedom and a p-value of 0.298, indicating no statistically significant association between staff role and reporting behavior. This suggests that reporting behavior does not vary meaningfully across job categories within public higher learning institutions in Tanzania.

Table 2: Chi-square Test of Role vs. Reporting Behavior

Variable	χ^2 (Chi-square)	df	p-value	Interpretation
Role × Reporting	9.55	8	0.298	Not statistically significant

From a theoretical standpoint, this finding aligns with the Socio-Technical Systems Theory, which emphasizes that human behavior in technological contexts is shaped more by the interaction of social norms, institutional support and systemic enablers than by formal job designation alone (Zoto et al., 2018; Semlambo, 2025). The result is consistent with Bada et al. (2019), who noted that systemic factors, such as fear of blame, lack of confidentiality and absence of clear policies often override individual characteristics like professional role. This reinforces the idea that improving incident reporting requires structural and cultural reforms rather than role-specific interventions. Leadership engagement, clear policies and anonymous reporting mechanisms may thus be more effective levers for change than targeting specific staff groups.

Chi-Square Test: Gender and Reporting Behavior

A Chi-square test was also conducted to assess whether there is a relationship between gender and incident reporting behavior. While not the main focus of the study, this analysis provides additional insight into possible demographic influences on reporting practices.

Similar to the role comparison, no significant difference was found in incident reporting behavior between male and female staff members (p > 0.05).

Table 3 shows the results of a Chi-square test assessing the relationship between gender and incident reporting behavior. The test produced a Chi-square value of 4.00 with 4 degrees of freedom and a p-value of 0.406, indicating no statistically significant association. This suggests that male and female staff are equally likely or unlikely to report ICT security incidents within the sampled institutions.

Table 3: Chi-square Test of Gender vs. Reporting Behavior

Variable	**χ^2 (Chi-square)**	**df**	**p-value**	**Interpretation**
Gender × Reporting	4.00	4	0.406	Not statistically significant

Table 4: Pearson Correlation Coefficients – Predictors of Reporting Behavior

Predictor Variable	**Correlation Coefficient (r)**	**Significance (p-value)**	**Interpretation**
Responsibility to report	0.18	0.061	Not significant
Knowledge of procedures	0.24	0.038*	Significant
Trust in confidentiality	0.29	0.021*	Significant
Fear of blame or punishment	-0.31	0.018*	Significant
Frequency of training	0.34	0.014*	Significant
Leadership support	0.36	0.010*	Significant
*p < 0.05			

This finding reinforces the Socio-Technical Systems Theory perspective, which posits that security behavior is shaped more by systemic and organizational factors than by individual demographic attributes (Zoto et al., 2018; Semlambo, 2025). It also aligns with the broader literature suggesting that while gendered experiences can influence perceptions of risk (Choi, 2016), reporting behavior itself is more heavily determined by institutional conditions, such as fear of blame, lack of confidentiality or unclear procedures (Bada et al., 2019; Park & Kim, 2020). The absence of a gender-based reporting gap highlights the need to focus on building trust and strengthening reporting structures for all staff, rather than tailoring interventions along gender lines.

Research Question 3: Is there a significant relationship between behavioral, organizational, and cultural factors and incident reporting behavior in Tanzanian public higher education institutions?

To further examine the relationship between behavioral, organizational and cultural factors and reporting behavior, a Pearson correlation analysis was conducted to determine whether variables such as perceived responsibility, knowledge of procedures, trust in confidentiality, fear of blame, training frequency and leadership relate with reporting behavior.

Table 4 presents the results of Pearson correlation analysis, examining the relationship between selected institutional and behavioral variables and incident reporting behavior. The results show that five out of six variables show a significant association with reporting behavior (p < 0.05), while one variable does not.

Trust in the confidentiality of the reporting process (r = 0.29, p = 0.021) and knowledge of procedures (r = 0.24, p = 0.038) also showed significant positive correlations. This suggests that when staff understand how to report and believe that their identity will be protected, they are more inclined to take action. These results are consistent with Choi et al. (2023) and Park and Kim (2020), who found that confidential and clearly communicated reporting systems are critical for encouraging disclosure in risk-sensitive environments.

Conversely, fear of blame or punishment had a significant negative correlation with reporting behavior (r = -0.31, p = 0.018), indicating that the more staff fear reprisals, the less likely they are to report incidents. This finding mirrors the conclusions of Adams and Sasse (2019) and Bada et al. (2019), who reported that punitive or unsupportive environments discourage open reporting and erode trust in institutional processes. Within the STS framework, this highlights a misalignment between policy expectations and the social context—particularly in how accountability and communication are handled within institutions.

Finally, the variable perceived responsibility to report (r = 0.18, p = 0.061) was not significant. While staff may recognize reporting as part of their duty, this perception alone does not appear sufficient to drive behavior unless supported by structural and cultural enablers. This underscores the STS perspective that individual awareness must be reinforced by systemic support for behavioral change to occur.

Conclusion and Recommendations

Conclusions

This study concludes that while staff generally recognize incident reporting as a professional responsibility, actual reporting behavior is hindered by fear of blame, limited trust in confidentiality, inadequate training and unclear procedures. Organizational enablers, such as leadership support, regular training and clear, confidential processes were significantly correlated with increased reporting. These results underscore the need for structural reforms that prioritize psychological safety, proactive leadership and user-centered policies to cultivate a strong reporting culture in resource-constrained academic environments.

Recommendation

To enhance ICT incident reporting in Tanzanian public higher learning institutions, the study recommends simplifying and decentralizing reporting mechanisms, including the option for anonymous submissions, to reduce fear of reprisal. Regular, mandatory training programs should be institutionalized to improve staff awareness and procedural clarity. Leadership must take an active, visible role in promoting a non-punitive reporting culture and consistently reinforcing the value of incident disclosure. ICT policies should be reviewed regularly through participatory processes, involving staff input to ensure contextual relevance and institutional ownership. Additionally, implementing feedback loops that inform reporters of follow-up actions can foster transparency, build trust and strengthen long-term engagement with formal reporting systems.

References

Adams, A. and Sasse, M. A. (2019). Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. Communications of the ACM, 62(9), 82–89.

Alqahtani and Kavakli (2022) Developing an Information Security Policy: A Case Study Approach. 4th Information Systems International Conference (pp. 691-697). Bali, : ISICO.

Alshaikh, M., Maynard, S. B., Ahmad, A. and Chang, S. (2021). Information Security Policy: A Management Practice Perspective. The 26th Australasian Conference on Information Systems (pp. 1-13). Adelaide: The 26th Australasian Conference on Information Systems.

Bada, M., Sasse, M. A. and Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.

Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.

Bryman, A. (2016). Social Research Methods (5th ed.). Oxford University Press.

Choi, M. (2016). Leadership of Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing. Sustainability , 8(7), 6-38.

Choi, S. H., Youn, J., Kim, K., Lee, S., Kwon, O. J. and Shin, D. (2023). Cyber-resilience evaluation methods focusing on response time to cyber infringement. Sustainability, 15(18), 13404.

Creswell, J. W. (2009). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (3rd ed.). Sage.

ENISA. (2020). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. European Union Agency for Cybersecurity.

Gundu, T. and Flowerday, S. (2020). The enemy within: A model for insider threat risk management. Computers & Security, 93, 101780.

Masrek, M. N. and Mohd Sam, M. F. (2017). Information security awareness and compliance: A case study of a public university in Malaysia. Education and Information Technologies, 22(6), 2825–2840.

Pahnila, S., Siponen, M. and Mahmood, M. A. (2015). Employees' behavior toward IS security policy compliance: A security culture perspective. Information & Computer Security, 23(2), 134– 154.
Park, H. and Kim, H. (2020). Trust and transparency in information security incident management. journal of Cybersecurity, 6(1), taaa001.

Rezgui, Y. and Marks, A. (2015). Information security awareness in higher education: An exploratory study. Computers & Security, 49, 67–75.

Semlambo, A. A. (2025). Safeguarding the Security of Information Systems through ICT Policies in Public Higher Learning Institutions in Tanzania [Doctoral dissertation, Open University of Tanzania].

Tanzania Computer Emergency Response Team (2023). *Annual cybersecurity threat bulletin*. Retrieved from https://www.tzcert.go.tz

Verizon. (2021). 2021 Data Breach Investigations Report. Verizon Enterprise.

Zoto, E., Kowalski, S., Lopez-Rojas, E. A., & Kianpour, M. (2018). Using a socio-technical systems approach to design and support systems thinking in cyber security education. STPIS'18 Workshop, 123–128.