https://doi.org/10.56279/orseaj.v15i2.7

IT Infrastructure and Employee Cybersecurity Awareness on Mitigation of Information Security Breaches in Higher Education Institutions

Wesimika Andrew[1], Manana Peter[2], Prisca Nabukwasi[3], Lydia Kimono[4] and Ismail Bumba[5]

Abstract

The research concentrated on how much IT infrastructure and cybersecurity awareness in the workforce can help decrease information security breaches in the Ugandan public higher education institutions. A cross-sectional design approach was adopted, with the data being collected between January and April 2025, with a sample size of 356 participants consisting of academic personnel, administrators, and ICT personnel. Analysis was done using partial least squares structural equation modelling (PLS SEM). The data indicated a clear and robust impact of employee cybersecurity awareness on the minimization of information security breaches (β =0.644, $p < 0.000$). IT infrastructure had a significant positive impact (although less than other minor effects), too (β = 0.152, $p < 0.001$). These two factors explained 54.2% of the difference in the mitigation of information security breaches (R2 = 0.542). The findings highlighted the need to focus on strategies for improving employee awareness of cybersecurity and investment in a well-developed IT infrastructure. Enhancing both human and technical aspects of security could also go a long way in improving the capacity of universities to avert, identify, and control computer threats. The evidence generated by this study informs policymakers and university managers in developing a comprehensive cybersecurity policy that balances the protection of both infrastructure and individuals.

Keywords: Information Security Breaches, Cyber Security, IT Infrastructure, Higher Education Institutions

Introduction

At the core of minimizing information security breaches in organizations is good IT infrastructure and cybersecurity-aware employees (Ajayi et al., 2025; Cheng & Wang, 2022). Research has shown that probably the biggest factor determining an organization's operational efficiency, innovation, and competitive advantage is a stable IT infrastructure (Feng & Ali, 2024). Increasingly, higher education institutions (HEIs) are using IT Infrastructure to support research, learning, administration, and interaction with stakeholders (Machaladze, 2025). It is important to note that Universities are notoriously being targeted as cyberattacks happen in frequency. According to the Verizon Data Breach Report (2024), the education sector accounted for 17% of analyzed global incidents, many of which resulted in data disclosure. Similarly, Check Point

[1] Makerere University Business School Mbale Campus, Uganda
Email: awesimika@mubs.ac.ug
[2] Makerere University Business School Mbale Campus, Uganda
[3] Makerere University Business School Mbale Campus, Uganda
[4] Makerere University Business School Mbale Campus, Uganda
[5] Makerere University Business School Mbale Campus, Uganda

Research (2024) reported that education and research institutions experienced an average of 3,006 cyber-attacks per organization per week, representing a 37% increase from the previous year. The increased vulnerability is largely attributed to the open-access nature of the IT infrastructure, which facilitates unauthorized access and cyberthreat penetration, as supported by studies conducted by (Lallie et al., 2025). Security breaches have catastrophic effects on the institution's integrity, and trust can be lost amongst students, staff, and external partners. Moreover, efforts to reduce information security breaches in institutions of higher learning are made even harder by the lack of standard IT Infrastructure and cybersecurity awareness among the employees (Rohan et al., 2025). The growing complexity of cyberthreats suggests the necessity of more than just technical training to respond to them. There is a need to be sensitized on possible cybersecurity threats, and individuals and organizations are not only supposed to be provided with technical knowledge, but also must be conscious and responsive to emerging threats. (Qudus, 2025; Moonsammy et al., 2024).

An IT infrastructure is a critical variable in addressing information security breaches (having a robust, well-established, and scalable infrastructure) (Ajayi et al., 2025; Khaustova et al., 2023). As much as infrastructure needs to improve, cybersecurity threats have elevated at the same time (Adebayo, 2023). In Africa, even though many higher education institutions have experienced digital growth, there is still limited knowledge on cybersecurity threats (Oroni et al., 2025). In the context of low-income countries like Uganda, efforts are underway to limit information security breaches. One option available is cyber security awareness campaigns (Mbonimpa et al., 2024), a need for existing gaps in cyber security policy (Andrew et al., 2025). Early evidence indicates that the majority of these breaches as a result of insufficient information technology infrastructure and limited awareness of cybersecurity practices from employees (Alzahrani, 2021). Despite the substantial body of research in the domain of IT Infrastructure and employee awareness that are fundamental to mitigating information security breaches, within the context of low income and resource constrained settings such as Uganda, there is lack of empirical PLS-SEM studies in Ugandan HEIs, limited integrated studies combining both IT infrastructure and employee awareness and lack of validated measurement instruments highlighting a critical and underexplored gap in existing literature on the role of IT Infrastructure and Cybersecurity awareness in terms of mitigating the occurrence of information security breaches (Yusuf, 2024; Bwiino et al., 2025). This study aims to bridge the gap through an integrated analysis of information security management in the context of HEIs in Uganda. The study further seeks to examine the role of IT Infrastructure and Employee cybersecurity awareness on the Mitigation of information security breaches in higher education institutions in Uganda. The analysis of the two dimensions will enable better comprehension of how organizational and human factors can be used to enable institutional susceptibility to information security. The results will influence the future policy, capacity building, and investment in the IT infrastructure towards enhancing the resilience to information security breaches in the Ugandan HEIs setting.

Theoretical review

Past studies have applied different information security theories and frameworks to address information security breaches (Kuppusamy, 2020). Although these traditional theories are applied to other environments, they fail to give appropriate attention to the complexities of the enduring information security breaches of the higher education settings. In dealing with the long-held problem of information security compromises at institutions of higher learning, the Technology

Organization Environment (TOE) presented by Tornatzky and Fleischer (1990) can provide a fairly resilient theoretical framework in understanding how internal organizational strengths interact with the influence of environmental factors on how institutions respond to security risks and embrace new practices. With particular reference to the technology dimension in the TOE context, IT infrastructure comprising hardware, software, networks, and systems integration is especially important for the pre-emptive detection, prevention, and management of security vulnerabilities. A developed IT infrastructure will unlock many forms of encryption, intrusion detection systems, and improvements to access controls that will reduce the instances of breaches and the severity of the challenges faced when responding to security incidents (George et al., 2024). On the organizational aspect, the notion of cybersecurity awareness is also applicable. The paper capitalizes on the major assumptions of the Unified Theory of Acceptance and Use of Technology (UTAUT) developed by (Venkatesh et al., 2003), which address the behavior of the user and acceptance of technology due to continuous training, repetitive institutional policies, and encouragement of the leadership to establish an institutional culture of vigilance and adherence (Chrzaszcz, 2024). Your technical controls against human error, which is generally considered the weakest link in cybersecurity protection of an institution, will also be complemented by the behavioral component (Tambe-Jagtap, 2023; Corradini, 2020). Combined, the three distinct TOE framework dimensions make the mitigation of information security breaches more than simply a technical exercise; the internal systems thinking involved should embrace the real capabilities, culture, and environment of the actual institution. Increasing IT capacity and raising awareness in the field of cybersecurity could allow higher education institutions to shift towards preventive information security management, rather than reactive, and increase resilience and reduce the operational consequences of security breaches (Folorunso, 2024).

Hypothesis development

When considering the factors in mitigating Information Security Breaches, it is easy to note that IT Infrastructure is a powerful factor (Li, 2021). According to recent research, the IT infrastructure capability is one of the key contributors to assist in overcoming the information security breach, especially in the complicated organizational setting like higher education (Odionu et al., 2024). The capabilities and components of an institution's IT infrastructure and features such as real-time monitoring, storage of data in secure computing facilities, operational and integration capabilities, positively influence the organization's demonstrated security posture (Malasowe et al., 2024). In higher education institutions, institutions with strong infrastructure are better positioned to exercise preventive controls, detect anomalies, and take swift preventive or remedial actions on security threats (Adebayo, 2024). However, as suggested by Sekara (2024), having sophisticated systems does not guarantee success unless it is with a strategic and risk-aware approach.

H_1: *IT Infrastructure has a positive effect on the mitigation of information security breaches in higher education institutions.*

Recent literature highlights the importance of security awareness to diminish breaches of information security, both in terms of frequency and effects, particularly in knowledge-intensive environments such as higher education institutions. Researchers such as Bwiino et al., (2025) argue that creating outcomes for organizations is not only determined by technology, but also relies on user skills, user attitude, and user awareness. This view aligns with research of (Li et al.,

2023), who even with the best sophisticated systems, will underperform if the users don't understand the system and the risks associated with user mistakes. In the context of Cybersecurity, many breaches can be attributed to human error, such as weak passwords, being susceptible to phishing attempts, and poor data handling practices, and making employee awareness and behavior a key component of institutional security (Al-Badayneh, et al., 2025). Moreover, Aksoy et al., (2024) argue that leadership-behavioral commitment to previous and ongoing training for staff in the operational use of digital systems creates a cyber cybersecurity resilience culture. As higher education institutions continue to use digital tools for administration, learning, and communication, it is essential to provide staff and faculty with the necessary knowledge and attitudes to effectively secure their digital practices. Employees unable to identify security protocols and keep current on evolving threats will be less likely to take prevention steps to avoid breaches or respond accordingly after a breach has occurred. From this synthesis of literature, the following hypothesis is suggested:

H_2: *Employee Cybersecurity Awareness has a positive effect on the mitigation of information security breaches in higher education institutions*

Methodology

Population and Sample

A cross-sectional quantitative survey design was employed to examine the relationships between the study variables at a single point in time (Slater & Hasson, 2025). The target group was 7,440 employees of the public universities of Uganda (UBOS Abstract report, 2023). The SurveyMonkey sample size calculator was used to set the minimum sample size at 366 respondents at a 95% confidence level and a margin of error set at 5. Purposive sampling was used to pick up the participants, as they were directly involved in IT management or data handling, or administration processes, as these participants were deemed to be the most informed about the practices of cybersecurity in institutions (Ali et al., 2025). Inclusion criteria meant that the participants had (i) worked at the institution for at least one year, (ii) had direct access to institutional IT systems or data, and (iii) were involved in day-to-day operations that required the use of IT. The process of data collection was done within the period of January 2025 to April 2025, and 366 questionnaires were given. The response rate was 97.3, and 356 valid responses were obtained after the elimination of non-responses and incomplete submissions. Admittedly, the low number of IT personnel (n=16) in the small sub-group restricted the applicability of results to the targeted group. Nonetheless, the sample of 356 respondents was adequate for analyzing overall relationships at a 95% confidence level and 5% margin of error. The high response rate strengthened its reliability.

Variable Measurement

IT infrastructure, employee cybersecurity awareness, and mitigation of information security breaches measurement items were modified based on previous validated studies (Adeusi et al., 2024; Abrahams et al., 2024; Gilbert et al., 2025). The measures of the items were determined on the basis of the 5-point Likert scale (1=strongly disagree to 5=strongly agree (Jeb et al., 2025). The pretest of the questionnaire was done on 20 members of staff who were not involved in the study to determine that the measures were clear, relevant, and reliable.

Data Analysis

The IT personnel, academic personnel, and administrative officers made up the unit of analysis in the institutions of higher learning. Descriptive statistics were generated using SPSS to provide a summary of important respondent characteristics like age, gender, staff category, tenure, and other demographic information. Both the measurement and structural models were analyzed with the help of the Partial Least Squares Structural Equation Modelling (PLS-SEM), being a sophisticated method suitable for multivariate analysis that can effectively address the needs of studying both reflective and formative indicators and both the measurement and structural models (Hanafia, 2020). The analytical process was based on two key steps of the measurement model estimation and structural model testing (Hair et al., 2025). In the measurement model analysis, reliability, validity, collinearity, and the contribution of each indicator were checked. The structural model analysis focused on the identification of the intensity and the direction of the influences between the constructs using path coefficients and the overall model evaluation (Kapoor, 2025).

Results and Discussion

According to Table 1, the majority of the respondents were men, forming up to 59.2% of the sample, and women represented 40.2%. The respondents who were above 50 years 22.2% indicated that a considerable fraction of the surveyed employees had extensive work experience in terms of staffing. The academic personnel had the highest percentage of all the respondents, 70.4%, 24.6% represented administrative staff, with the IT officers at 4.5% of the respondents. Regarding the number of years at the institution, 40.7% of the respondents served a period between 1 to 4 years, 33.4% served a period between 5 to 7 years, 19.4% served a period between 8 to 10 years, 3.1% served a period between 11-13 years, and 3.4% served above 13 years. In general, the sample was balanced in terms of the work experience and years of service in the institutions involved.

Table 1: Demographic Characteristics

Variable	Category	Frequency	Percent (%)
Gender	Male	212	59.2
	Female	144	40.2
Age	18-25	7	2.0
	26-33	110	30.9
	34-41	82	23.0
	42-49	78	21.9
	50+	79	22.2
Employee Category	IT staff	16	4.5
	Academic Staff	252	70.4
	Administrators	88	24.6
Years In the Organization	1-4	145	40.7
	5-7	119	33.4
	8-10	69	19.4
	11-13	11	3.1
	13+	12	3.4
Total	-	356	100.0

Source: *Primary data (2025)*

Measurement Model Assessment

Testing of the measurement model was done to find out how valid and reliable the variables were. Both convergent and discriminant validity were considered in the process. For convergent validity testing, factor loadings and average variance extracted (AVE) were considered, indicating how accurately each measurement item was reflected (Ghazali et al., 2025). Discriminant validity was utilized, namely having met the Fornell-Larcker and Heterotrait-Monotrait (HTMT) criteria, with all values within the acceptable limits (Mirhosseini et al., 2025). **Table 2** shows that all factor loadings were greater than 0.70, demonstrating the items' validity is acceptable. Further, the average variance extracted meets the established threshold minimums > 0.5. Additionally, In **Table 2**, for composite reliability, the least score across all variables was 0.830, exceeding the significant threshold minimum of > 0.70 (Hair et al., 2025). Variance Inflation Factor (VIF) was used to measure whether collinearity exists among the indicators. Table 2 displays, all VIF values were well below the common thresholds of 3.3, indicating that multicollinearity was not an issue in the model. As well as, in Table 3, although the Fornell and Larcker criteria measures discriminant validity sufficiently, we additionally measured discriminant validity by examining the Heterotrait-Monotrait measures to refute valid criticisms that empirical evidence that indicate the Fornell and Larcker criteria cannot measure discriminant validity when indicator loadings of a construct differ by a couple of points (Cheung et al., 2024). All of the Heterotrait-Monotrait (HTMT) ratios were less than 0.9, indicating strong discriminant validity and high internal consistency among the construct items.

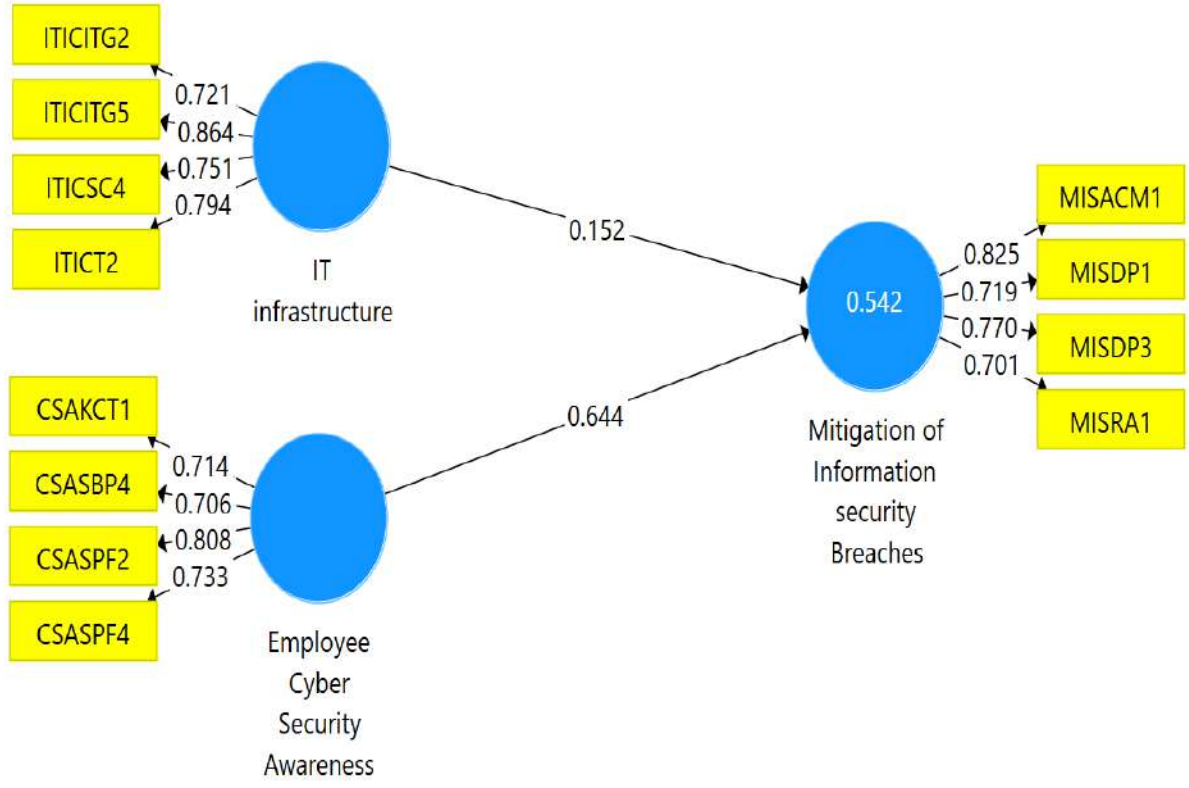

Figure 1: Measurement Model

Table 2: Lower-Order Measure of Construct Validity and Reliability

Constructs	Codes	FL	CA	CR	AVE	VIF
IT Infrastructure	ITIITG2	0.721	0.745	0.830	0.550	1.145
	ITIITG5	0.864				1.769
	ITISC4	0.751				1.803
	ITIT2	0.794				2.248
Employee Cybersecurity awareness	CSAKCT1	0.714	0.800	0.864	0.615	1.618
	CSASBP4	0.706				1.587
	CSASPF2	0.808				1.523
	CSASPF4	0.733				1.960
Mitigation of information security breaches	MISACM1	0.825	0.761	0.841	0.571	2.555
	MISDP1	0.719				1.726
	MISDP3	0.770				2.080
	MISRA1	0.740				1.105

Source: *Primary data (2025)*

Discriminant Validity and Measurement Model Assessment

The discriminant validity was tested with both Fornell Larker criterion and Heterotrait-Monotrait (HTMT) ratio. According to the Fornell-Larcker results, the square root of the AVE of each construct was larger than the correlations of the constructs with others, which indicated good discriminant validity with (ITI=0.784), (MISB=0.755), and (CSA=0.741). All the values of the HTMT were less than the 0.90 threshold, and (ITI-CSA=0.526, ITI-MISB=0.567, and CSA-MISB=0.825) indicate that the constructs are empirically different (Wingate et al.,2025). This means that the constructs adopted in the research were appropriate in the analysis of the structural model that followed. The Value (0.152) of SRMR is above the recommended value of 0.08, which indicates a less appropriate model fit (Sunarti et al., 2025). Nonetheless, PLS-SEM is more concerned with predictive accuracy, but not a perfect fit of the model (Hair et al., 2025). This implies that SRMR gives valuable information but is not decisive, but complementary to it, where more importance is given to predictive relevance (Q^2) and the importance of path coefficients. The predictive relevance of the model was determined by the procedure known as blindfolding, and it was found that the Q^2 value was 0.262. This is larger than zero, which is why it shows that the model has good predictive ability (Hair et al., 2025). The structural model also showed that the influence of IT Infrastructure on Employee Cybersecurity Awareness was also insignificant ($f^2 = 0.036$, $p > 0.05$), which implies that the level of employee awareness cannot be improved through the improvement of IT infrastructure only. On the other hand, the Information Security Management was significantly and statistically affected by IT Infrastructure ($f^2 = 0.653$, $p < 0.001$), which means that a well-developed IT infrastructure contributes a lot to the enhancement of information security practices in HEIs.

Table 3: Discriminant Validity and Measurement Model Assessment Results

		ITI	CSA	MISB	F^2	Q^2	SRMR
		Values					
					0.036	0.262	0.152
Fornell-Larcker	IT Infrastructure (ITI)	0.784	0.529				
	Employee Cybersecurity Awareness (CSA)		0.741				

	Mitigation of Information Security Breaches (MISB)	0.493	0.725	0.755			
		ITI	CSA	MISB			
Heterotrait-Monotrait (HTMT 0.9)	IT Infrastructure (ITI) Employee Cybersecurity Awareness (CSA) Mitigation of Information Security Breaches (MISB)	 0.526	0.567 0.825				

Source: *Primary data (2025)*

Structural Model Assessment

The R^2 statistic was utilized to determine how well the proposed IT Infrastructure and cyber security awareness explain the variation efforts to mitigate information security breaches. The R^2 statistic resulted in a R^2 statistic of 0.542 for IT Infrastructure and cyber security awareness, indicating that the IT Infrastructure and cyber security awareness explain 54.2% of the variance in mitigation of information security breaches. In addition, the proposed hypotheses were tested with 5,000 replicates using a non-parametric bootstrapping method (Mougan et al., 2023). There were significant effects of IT Infrastructure (0.152, $p<0.001$), cyber security awareness (0.644, $p<0.000$), on the mitigation of information security breaches therefore, supporting the hypothesis. Results shown in Table 4 demonstrate that IT Infrastructure and cybersecurity awareness are significant factors influencing the mitigation of information security breaches in higher education institutions. Nonetheless, the confidence intervals reported (2.5% and 97.5%) indicate a two-tailed test. In PLS-SEM, when bootstrapping is used to assess path coefficients, the 95% confidence interval is calculated to determine if the effect is statistically significant.

Table 4: Path Effects Results

Direct Path Coefficient							Supported/ Not supported
Hypothesis	Relationship	β	T Value	P Value	Confidence Interva 2.5%	Confidence Interval 97.5%	
H1	IT Infrastructure ->mitigation of information security breaches in higher education institutions	0.152	3.389	0.001	0.069	0.242	Supported
H2	Employee Cyber Security Awareness->mitigation of information security breaches in higher education institutions	0.644	20.414	0.000	0.583	0.702	Supported

Construct	R2	Adjusted R2
Mitigation of Information Security Breaches in Higher Education Institutions	0.542	0.539

Source: *Primary data (2025)*

AVE: Average variance extracted, CR: Composite reliability, and FL: Factor Loadings are significant at p < 0.001 level.

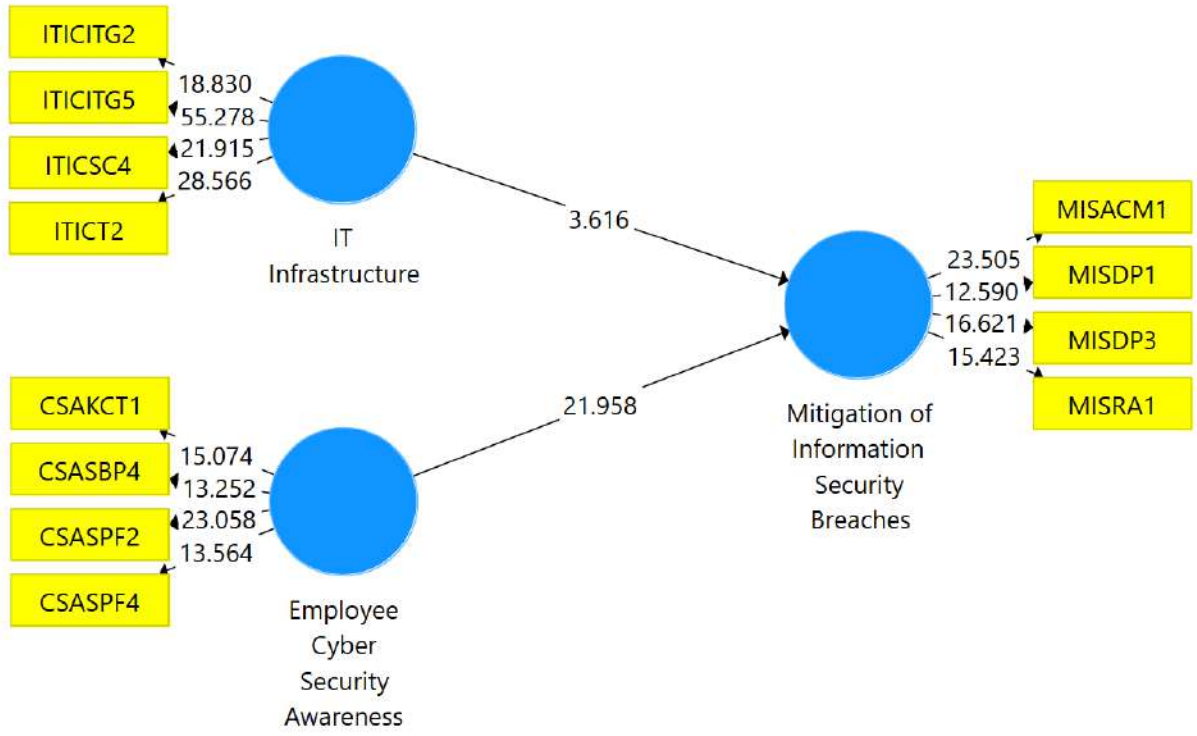

Figure 2: Structural Model Depicting the Hypothesized Relationships and Empirical Findings

The study investigated the effects that IT Infrastructure and cybersecurity awareness have on the mitigation of information security breaches in higher education institutions. The study was based on the Technology-Organization-Environment (TOE) framework (Tornatzky & Fleischer, 1990) and the unified theory of acceptance and use of technology (Venkatesh et al., 2003). The hypotheses formulated above were validated through data findings for H1 and H2 in support of the proposed relationship, which determined that the influence and impact that IT Infrastructure and cybersecurity awareness have on the mitigation of information security breaches in higher education institutions are statistically significant. In consideration of the data findings, (Figure 1). The two predictor variables, IT Infrastructure and employee cybersecurity awareness, jointly explained 54.2% (R^2=0.542) of the variance in mitigation of information security breaches, indicating a moderate explanatory power of the model.

The debate about what preemptive measures to take as a mitigation strategy for information security breaches in higher education institutions is ongoing. Research by Ayedh et al., (2023) has continued to encourage factors such as access control measures, data protection, and periodic information security audits; however, many higher education institutions, especially in developing countries, have still exhibited a high rate of information security breaches that can ultimately impact on the security position of the institution. This study contributes to the debate by establishing the presence of IT Infrastructure in the mitigation of information security breaches. The results show that technology standardization, system integration and scalability, and information technology governance have a significant impact on the mitigation efforts to reduce information security breaches. This was supported by Ahmed et al., (2022), who state that with good and updated IT Infrastructure, information security breach mitigation efforts won't be in vain. In addition, Merchan-Lima et al., (2021) have also supported the idea that institutions can improve security posture through improving IT Infrastructure.

In reference to hypothesis H_2, the results revealed that employee cyber security awareness has a significantly positive relationship with information security breaches mitigation. This means that if the level of cybersecurity awareness is increased among employees of HEIs, then the organization's ability to mitigate information security breaches will also improve significantly. In the Ugandan context, Mbonimpa, (2024) has shown that institutions that have actively engaged in training their employees on the mitigation strategies of information security breaches have more ability to limit the number of breaches that they experience based on their levels of awareness. In support of the findings, Olabode, (2023) stated that organizations that have well-trained and well-informed employees will be far more valuable, in regard to their application of objective and realistic solutions to information security breach issues. The results also suggest that employees' knowledge of cybersecurity ethics, familiarity with security policy, and secure behavior practices are positively related to the mitigation of information security breaches. The relationship also indicates that IT Infrastructure integrates with employee cyber security awareness; therefore, mitigation of information security breaches can only be reinforced when cultivating a culture of awareness into a matrix that inherently brings cyber security awareness and IT Infrastructure together as an effort to modernize these institutions, along with global standards.

There is also the realization that an integration of IT Infrastructure with cybersecurity awareness has a positive effect on mitigating information security breaches, which creates a safer and secure work environment to conduct operations, which has the effect of improving the overall information security posture of the institutions. Therefore, ensuring institutions are establishing sound IT Infrastructure while also providing cybersecurity awareness training, containing what employees should know about cybersecurity ethics, security policy familiarity, and security behavior practice. This supports a culture of sound IT Infrastructure, cybersecurity knowledge, and a sustainable process with updated IT Infrastructure using cybersecurity awareness training to enforce information security breaches mitigation in HEIs to do a better job of screening data to avoid breaches of security.

Conclusion and Implications

This study examined the effect of IT Infrastructure and Employee cybersecurity awareness on information security breaches mitigation in HEIs. The findings indicated that IT Infrastructure, assessed through technology standardization, system integration, scalability, and information technology governance, positively affects the mitigation of information security breaches. In addition, the study iterates that cybersecurity awareness, particularly related to secure behavior practice, security policy awareness, and knowledge of cybersecurity threats, plays a role in the efforts to mitigate information security breaches. The study is also a contribution to the body of knowledge since it concentrates on IT infrastructure and Employee cybersecurity awareness in a specific context of Uganda's higher education institutions, which is a less-examined area of study. This study differs from previous research by considering dimensions of behavior and technology in the analysis of information security breaches mitigation, providing a more systemic perspective in its own right. For industry practitioners in higher education institutions, the key findings demonstrate a duty to provide updated IT infrastructure and cybersecurity awareness for timely information security breach mitigation strategies. In line with research by Fagbule, (2023), Companies investing in IT infrastructure and employee cyber security awareness training provide a culture of mitigation strategies with the relevant stakeholders that facilitate, create a safe and smooth operating environment by improving risks associated with information security breaches.

Nonetheless, for regulators and policymakers, the insights are used to devise a framework to strengthen information security breach mitigation strategies in higher education institutions. Policies that value employee education and compliance with information technology standards are gradually enhanced for mitigation strategies of information security breaches. The study is more significant, as it established that information security breach mitigation strategies in higher education institutions are enabled by IT Infrastructure but are shaped by employees' cybersecurity awareness. In lay terms, instead of relying on old methods of information security breach mitigation, organizations should seek to leverage IT Infrastructure with the competence of the employee using cybersecurity awareness to respond to the challenges encountered. Studies carried out by Keefa et al., (2024) emphasize continued efforts in information security audits, protection of data, and access controls to ensure a smooth and sustainable operation, hence encouraging policymakers, industry leaders, and academics to work together to generate insights on strengthening the security posture of their institutions in Uganda and beyond.

Recommendations

University councils and IT boards prioritize clear governance instruments to establish cybersecurity strategies, not forgetting proper budgeting and compliance audit reports. Updated IT systems are highly recommended for the reduction in rates of system failures and unprecedented cyberattacks. Customized information security awareness training to staff and students should be conducted in an effort to minimize abrupt threats to the university's IT infrastructure. Promote a culture of safety in the workplace through improved leadership communication and offering rewards for compliance efforts by staff. National information security bodies should collaborate with higher education institutions to harmonize information security requirements for quicker and swifter responses to potential cyber threats.

References

Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: A review of employee engagement and accountability. *Computer Science & IT Research Journal, 5*(1), 100–119. https://doi.org/10.51594/csitrj.v5i.708

Adebayo, O. S. (2023, March). *Cyber-attacks and impacts on the educational cyber infrastructures* [Paper presentation]. 17th Annual Research Dissemination Conference 2023, Mbarara University of Science and Technology, Mbarara, Uganda.

Adeusi, O. C., Adebayo, Y. O., Ayodele, P. A., Onikoyi, T. T., Adebayo, K. B., & Adenekan, I. O. (2024). IT standardization in cloud computing: Security challenges, benefits, and future directions. *World Journal of Advanced Research and Reviews, 22*(3), 2050–2057. https://doi.org/10.30574/wjarr

Ahmed, S., Ahmed, I., Kamruzzaman, M., & Saha, R. (2022). Cybersecurity challenges in IT infrastructure and data management: A comprehensive review of threats, mitigation strategies, and future trend. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology, 1*(01), 36–61. https://doi.org/10.62304/jieet.v1i01.228

Ajayi, O. O., Alozie, C. E., & Abieba, O. A. (2025). Enhancing cybersecurity in energy infrastructure: Strategies for safeguarding critical systems in the digital age. *Trends in Renewable Energy, 11*(2), 201–212. https://doi.org/10.17737/tre.2025.11.2.00192

Aksoy, C. (2024). Building a cyber security culture for resilient organizations against cyberattacks. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi, 7*(1), 96–110. https://doi.org/10.33416/baybem.1374001

Al-Badayneh, D. M., Al-Badayneh, D. D., & Hashish, R. K. (2025). Human factors of cybersecurity. *Journal of Posthumanism, 5*(4), 1302–1314. https://doi.org/10.63332/joph.v5i4.1242

Ali, A. B. A., Ayyasamy, R. K., Akbar, R., Jebna, A. K., & Adnan, K. (2025). Cybersecurity infrastructure compliance key factors to detect and mitigate malware attacks in SMEs: A systematic literature review. *SAGE Open, 15*(1). https://doi.org/10.1177/21582440251314671

Alzahrani, L. (2021). Statistical analysis of cybersecurity awareness issues in higher education institutes. *International Journal of Advanced Computer Science and Applications, 12*(11), 630–637. https://doi.org/10.14569/IJACSA.2021.0121172

Andrew, W., Adebayo, O. S., Peter, M., & Faisal, M. (2025). Improved Bring Your Own Device policy framework for mitigation of malware threats in higher institutions of learning. *Cybersecurity and Privacy*. https://doi.org/10.59232/CYS-V3I1P101

Ayedh, M. A. T., Wahab, A. W. A., & Idris, M. Y. I. (2023). Systematic literature review on security access control policies and techniques based on privacy requirements in a BYOD environment: State of the art and future directions. *Applied Sciences, 13*(14), 8048. https://doi.org/10.3390/app13148048

Bwiino, K., Mayoka, G. K., Nkamwesiga, L., & Nyamadi, M. (2025). Information security behavior in higher education institutions: A systematic literature review. *Journal of Information Security and Cybercrimes Research, 8*(1), 43–62.

Check Point Research. (2024). *Cyber security report 2024*. Check Point Software Technologies Ltd.

Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information, 13*(4), 192. https://doi.org/10.3390/info13040192

Cheung, G. W., Cooper-Thomas, H. D., Lau, R. S., & Wang, L. C. (2024). Reporting reliability, convergent and discriminant validity with structural equation modeling: A review and best practice recommendations. *Asia Pacific Journal of Management, 41*(2), 745–783. https://doi.org/10.1007/s10490-023-09871-y

Chrząszcz, A., Tomaszycki, M., Załoga, W., & Sztandera, A. (2024). The role of organizational culture in managing organizational security. *European Research Studies Journal, 27*(S1). https://doi.org/10.35808/ersj/3531

Corradini, I. (2020). Security: Human nature and behaviour. In *Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology* (pp. 23–47). Springer. https://doi.org/10.1007/978-3-030-43999-6_2

Fagbule, O. (2023). *Cyber security training in small to medium-sized enterprises (SMEs): Exploring organisation culture and employee training needs* [Doctoral dissertation, Bournemouth University]. Bournemouth University Repository.

Feng, C., & Ali, D. A. (2024). The impact of digital transformation on optimising organisational efficiency. *Accounting and Corporate Management, 6*(2), 109–115. https://doi.org/10.23977/acccm.2024.060214

Folorunso, A. (2024). Cybersecurity and its global applicability to decision making: A comprehensive approach in the university system. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4955601

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal, 2*(1), 51–75. https://doi.org/10.5281/zenodo.10639463

Ghazali, M. T., & Fauzi, M. A. (2025). Validation of training in relation to succession planning: Exploratory factor analysis and confirmatory factor analysis approach. *International Journal of Research and Innovation in Social Science, 9*(1), 785–798. https://doi.org/10.47772/IJRISS.2025.9010067

Gilbert, C., & Gilbert, M. A. (2025). Impact of General Data Protection Regulation (GDPR) on data breach response strategies (DBRS). *International Journal of Research and Innovation in Social Science, 9*(14), 760–784. https://doi.org/10.47772/IJRISS.2025.914MG0061

Hair, J. F., Babin, B. J., Ringle, C. M., Sarstedt, M., & Becker, J. M. (2025). *Covariance-based structural equation modeling (CB-SEM): A SmartPLS 4 software tutorial*. https://doi.org/10.1057/s41270-025-00414-6

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2025). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). Sage Publications.

Hanafiah, M. H. (2020). Formative vs. reflective measurement model: Guidelines for structural equation modeling research. *International Journal of Analysis and Applications, 18*(5), 876–889. https://doi.org/10.28924/2291-8639-18-2020-876

Jebb, A. T., Ng, V., & Tay, L. (2021). A review of key Likert scale development advances: 1995–2019. *Frontiers in Psychology, 12*, 637547. https://doi.org/10.3389/fpsyg.2021.637547

Kapoor, S. (2025, May). The role of SmartPLS in optimizing statistical analysis: A case study approach. In *2025 5th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)* (pp. 1–5). IEEE. https://doi.org/10.1109/IRASET64571.2025.11008204

Keefa, B., Mayoka, G. K., Nkamwesiga, L., & Nyamadi, M. (2024). Information security in higher education institutions: A systematic literature review. *ORSEA JOURNAL*, 302–320. https://doi.org/10.56279/orseaj.C2024.18

Khaustova, V., Tirlea, M. R., Dandara, L., Trushkina, N., & Birca, I. (2023). Development of critical infrastructure from the point of view of information security. *Univers Strategic, 1*, 5–16.

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration, 11*(4), 1–10. https://doi.org/10.4018/ijec.2015100101

Kuppusamy, P., Samy, G. N., Maarop, N., Magalingam, P., Kamaruddin, N., Shanmugam, B., & Perumal, S. (2020, June). Systematic literature review of information security compliance behavior theories. In *Journal of Physics: Conference Series* (Vol. 1551, No. 1, p. 012005). IOP Publishing. https://doi.org/10.1088/1742-6596/1551/1/012005

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyber attacks and cyber security vulnerabilities in the university sector. *Computers, 14*(2), 49. https://doi.org/10.3390/computers14020049

Li, H., Yoo, S., & Kettinger, W. J. (2021). The roles of IT strategies and security investments in reducing organizational security breaches. *Journal of Management Information Systems, 38*(1), 222–245. https://doi.org/10.1080/07421222.2021.1870390

Li, W. W., Leung, A. C. M., & Yue, W. T. (2023). Where is IT in information security? The interrelationship among IT investment, security awareness, and data breaches. *MIS Quarterly, 47*(1), 317–342. https://doi.org/10.25300/MISQ/2022/15713

Machaladze, O. (2025). IT infrastructure management in educational institutions using the ITIL framework. *International Science Journal of Engineering & Agriculture, 4*(2), 215–225. https://doi.org/10.46299/j.isjea.20250402.14

Malasowe, B. O., Aghware, F. O., Okpor, M. D., Edim, E. B., Ako, R. E., & Ojugo, A. A. (2024). Techniques and best practices for handling cybersecurity risks in educational technology (EdTech). *NIPES-Journal of Science and Technology Research, 6*(2). https://doi.org/10.5281/zenodo.12617068

Mbonimpa, T., Richard, N., Innocent, M. J., & Priscilla, M. (2024). Investigating security awareness and incident reporting levels at Mbarara University of Science and Technology. *Indonesian Journal of Innovation and Applied Sciences, 4*(3), 208–216. https://doi.org/10.47540/ijias.v4i3.1482

Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G., & Quiroz, D. (2021). Information security management frameworks and strategies in higher education institutions: A systematic review. *Annals of Telecommunications, 76*(3), 255–270. https://doi.org/10.1007/s12243-020-00783-2

Mirhosseini, S., Sharif-Nia, H., Gharehbaghi, M., Minaei-Moghadam, S., Obbels, J., Imani Parsa, F., & Ebrahimi, H. (2025). Psychometric evaluation of the Farsi version of the electroconvulsive therapy related anxiety questionnaire. *BMC Psychiatry, 25*(1), 729. https://doi.org/10.1186/s12888-025-07169-5

Moonsammy, A., Ahmed, M., Guidetti, O., & Rashid, B. (2024). Integrating human factors and systemic resilience: An interdisciplinary approach to cybersecurity in critical infrastructures and utilities. In *Psybersecurity* (pp. 1–34). CRC Press. https://doi.org/10.1201/9781032664859-1

Mougan, C., & Nielsen, D. S. (2023, June). Monitoring model deterioration with explainable uncertainty estimation via non-parametric bootstrap. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 37, No. 12, pp. 15037–15045). https://doi.org/10.1609/aaai.v37i12.26755

Odionu, C. S., Adepoju, P. A., Ikwuanusi, U. F., Azubuike, C., & Sule, A. K. (2024). The role of enterprise architecture in enhancing digital integration and security in higher education. *International Journal of Engineering Research and Development, 20*(12), 392–398. http://www.ijerd.com/vol20-issue12/2012392398.pdf

Olabode, O. (2023). *The relevance of cybersecurity awareness training for employees in small and medium enterprises (SMEs)* [Unpublished manuscript].

Oroni, C. Z., Xianping, F., Ndunguru, D. D., & Ani, A. (2025). Cyber safety in e-learning: The effects of cyber awareness and information security policies with moderating effects of gender and experience levels among e-learning students. *Education and Information Technologies*. Advance online publication. https://doi.org/10.1007/s10639-025-13366-2

Qudus, L. (2025). Advancing cybersecurity: Strategies for mitigating threats in evolving digital and IoT ecosystems. *International Research Journal of Modern Engineering and Technology and Science, 7*(1), 3185–3195. https://doi.org/10.56726/IRJMETS66504

Rohan, R., Chutimaskul, W., Roy, R., Hautamäki, J., Funilkul, S., & Pal, D. (2025). Developing a scale for measuring the information security awareness of stakeholders in higher education institutions. *Education and Information Technologies*. Advance online publication. https://doi.org/10.1007/s10639-024-13307-5

Sekara, H. P. (2024). *Strengthening cybersecurity culture using a systems security engineering approach to manage risks in emerging systems* [Doctoral dissertation, Marymount University]. ProQuest Dissertations and Theses Global.

Slater, P., & Hasson, F. (2025). Quantitative research designs, hierarchy of evidence and validity. *Journal of Psychiatric and Mental Health Nursing, 32*(3), 656–660. https://doi.org/10.1111/jpm.13135

Sunarti, T., Suprapto, N., Hidaayatullaah, H. N., Admoko, S., & Jauhariyah, M. N. R. (2025). Evaluating student responses to ethnophysics learning: Improving scientific literacy and problem-solving skills using a PLS-SEM approach. *Multidisciplinary Science Journal, 7*(10), 2025454. https://doi.org/10.31893/multiscience.2025454

Tambe-Jagtap, S. N. (2023). Human-centric cybersecurity: Understanding and mitigating the role of human error in cyber incidents. *SHIFRA, 2023*, 53–59.

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478. https://doi.org/10.2307/30036540

Verizon. (2024). *2024 data breach investigations report*. Verizon Communications Inc.

Wingate, T. G., Bourdage, J. S., & Steel, P. (2025). Evaluating interview criterion-related validity for distinct constructs: A meta-analysis. *International Journal of Selection and Assessment, 33*(1), e12494. https://doi.org/10.1111/ijsa.12494

Yusuf, A. A. (2024). *Employees' cybersecurity awareness and behaviour in South African higher education institutions* [Master's thesis, University of Pretoria]. University of Pretoria Research Data Repository. https://doi.org/10.25403/UPresearchdata.26311141.v1