Asia Pacific Science Press

Asia Pacific Economic and Management Review
ISSN(O):3005-9275
ISSN(P):3005-9267
Vol. 3 No.5 (2026)

People before Perimeters: Employee Awareness as the Primary Driver of Zero-Trust Architecture Adoption in Banking

Deogratius Mathew Lashayo*

Department of Computer Science, The Institute of Finance Management (IFM), Tanzania

Corresponding author: Deogratius Mathew Lashayo, deogratius.lashayo@ifm.ac.tz

Abstract: Financial institutions face increasing exposure to sophisticated cyber threats, prompting a shift from traditional perimeter-based security toward Zero-Trust Architecture (ZTA), a model built on continuous verification and least-privilege access. Despite growing global adoption, empirical evidence on the determinants of ZTA adoption within African, and more specifically Tanzanian, banking institutions remains scarce. This study examines the factors influencing ZTA adoption at NMB Bank PLC, Tanzania, using an extended Technology–Organization–Environment (TOE) framework augmented with an employee awareness construct. A quantitative, cross-sectional research design was employed, with data collected from 114 respondents and analyzed using multiple regression. Results indicate that technological readiness ($\beta = .224$, $p = .021$) and employee awareness ($\beta = .673$, $p < .001$) significantly and positively influenced ZTA adoption, with awareness emerging as the strongest predictor overall. Organizational factors ($\beta = -.136$, $p = .343$) and environmental/regulatory factors ($\beta = -.009$, $p = .964$) did not show statistically significant effects. These findings suggest that ZTA adoption in this context is currently driven more by human-capital readiness than by institutional or regulatory pressure, extending the TOE framework's applicability while highlighting its limitations for security technologies whose effectiveness depends on continuous human behaviour. The study offers empirical grounding for prioritizing awareness-building initiatives alongside technological investment in similarly positioned financial institutions, and contributes one of the first empirical assessments of ZTA adoption determinants within a Tanzanian banking context.

Keywords: Zero-Trust Architecture (ZTA); Technology-Organization-Environment (TOE) Framework; Employee Awareness; Cybersecurity Adoption; Financial Institutions; Tanzania

Published: Sep 3, 2026

DOI: https://doi.org/10.62177/apemr.v3i5.1638

1. Introduction

Commercial banks in developing countries are experiencing a growing volume of cyber-attacks, with financial institutions consistently identified as a primary target. Industry reports indicate that 28% of global cyber incidents target banks, and African financial institutions experienced a 30% rise in attacks in 2022; within this trend, roughly a third of recorded attacks targeting the region were directed at Tanzanian commercial banks[1]. This sustained increase has compelled banks to pursue a range of cybersecurity solutions in order to remain resilient against attacks, and the pattern suggests a steady and continuing growth of cyber threats facing commercial banks in developing countries generally.

Zero-Trust Architecture (ZTA) is one of the modern solutions increasingly used to prevent cyber-attacks, and it is particularly well suited to sensitive environments such as financial institutions, where it enhances security by design. ZTA is characterized by five core principles: (i) continuous verification, whereby identity and context are re-checked throughout a session rather than only at login; (ii) least-privilege access, whereby users and systems are granted only the minimum access necessary to perform their duties, and only for as long as needed; (iii) micro-segmentation, whereby the network is divided into small, isolated zones so that a compromise in one segment cannot easily spread to others (containing lateral movement); (iv) an assume-breach posture, whereby the architecture is designed on the premise that an attacker may already be inside the network, so that internal traffic is scrutinized as closely as external traffic; and (v) strong identity and access management (IAM), enforced through multi-factor authentication (MFA), device posture checks, and granular access policies[2].

Although ZTA technology exists and is increasingly promoted, relatively few commercial banks have fully installed and operationalized it, and few studies—globally, and in Tanzania particularly—have investigated the determinants of ZTA adoption, despite the framework's potential to meaningfully reduce cyber-attacks in sensitive institutions such as banks. While ZTA is fundamentally an Information and Communication Technology (ICT)-based innovation, its distinguishing features, outlined above, set it apart from other ICT-based technologies, meaning that determinants identified for the adoption of other technologies may not directly transfer to ZTA. The central research question motivating this study is therefore: what are the determinants of ZTA adoption in commercial banks in Tanzania? To answer this question, the study addresses the following specific research questions:

RQ1: To what extent does technological readiness (IAM maturity, network segmentation, authentication tooling) influence ZTA adoption at commercial banks?

RQ2: To what extent do organizational factors (leadership commitment, policy alignment, resource availability) influence ZTA adoption?

RQ3: To what extent do environmental/regulatory factors (Bank of Tanzania guidance, industry pressure, competitive climate) influence ZTA adoption?

RQ4: To what extent does employee awareness of ZTA principles influence its adoption?

Answering these four research questions is significant because each isolates a distinct, actionable lever for bank leadership, rather than treating "ZTA adoption" as a single undifferentiated outcome. Establishing the influence of technological readiness clarifies whether existing Identity and Access Management (IAM)—the framework of policies, processes, and technologies that ensures the right individuals and systems have appropriate access to the right resources at the right times, through functions such as authentication, authorization, and continuous monitoring—along with network segmentation and authentication infrastructure, is genuinely sufficient or remains a binding constraint on further investment. Determining the effect of organizational factors reveals whether leadership commitment and formal policy are translating into operational reality, since policies that exist on paper but are not operationalized represent a governance gap that technology spending alone cannot close. Isolating the influence of environmental and regulatory factors tests a widely held assumption in the adoption literature—that regulatory pressure and industry norms are primary adoption drivers—against empirical evidence from a specific Tanzanian institutional context, with direct implications for how the Bank of Tanzania and similar regulators calibrate cybersecurity guidance. Finally, answering the question of employee awareness carries particular weight because awareness and understanding sit at the intersection of the other three factors, since technology, policy, and regulation are all ultimately mediated by whether the people using and administering these systems correctly apply Zero-Trust principles day to day; if awareness proves to be the dominant predictor, the primary point of intervention shifts from procurement toward human-capital development and behavioural change management. Collectively, resolving all four questions together allows the study to move beyond simply confirming that ZTA adoption is multi-factorial—a claim broadly accepted in the literature—to precisely ranking which factors matter most in practice, the specific empirical contribution needed to guide where financial institutions, particularly in similarly under-resourced regional banking contexts, should direct scarce security investment for the greatest resilience gains.

The remainder of this manuscript is organized as follows: Section 2 reviews the theoretical and empirical literature on ZTA

adoption and develops the study's hypotheses; Section 3 describes the research methodology; Section 4 presents the results, discussion, and implications; and Section 5 concludes with recommendations and directions for future research.

2. Literature Review

2.1 Usage of Zero-Trust Architecture

Globally, financial services has emerged as the leading sector in Zero-Trust Architecture adoption. Industry analysis places financial-services adoption at approximately 50%, ahead of healthcare at 35% and manufacturing at 25%, a gap attributed to strict regulatory requirements and the high value of the data banks protect[1]. Adoption has accelerated markedly in recent years: the proportion of organizations worldwide that have launched a zero-trust initiative rose from 24% in 2021 to 61% in 2026[3]. Despite this momentum, a persistent execution gap remains, as 82% of organizations now regard zero-trust as essential to their security strategy, yet only around 17% report full implementation[1]. Large global banks illustrate the leading edge of this curve; institutions such as JPMorgan Chase and Goldman Sachs have incorporated core Zero-Trust components, including multi-factor authentication, network micro-segmentation, and continuous threat monitoring, to safeguard sensitive data and critical infrastructure[4]. The financial rationale for adoption is increasingly well documented: organizations with zero-trust architecture in place saved an average of US$1.76 million per breach compared with those without it, according to IBM's 2025 Cost of a Data Breach Report[5], and within banking specifically, zero-trust adoption has been associated with reducing the average dwell time of insider threats from 38 days to 4.2 days, an 89% improvement[6].

Within Tanzania and the wider East African and Sub-Saharan banking context, Zero-Trust Architecture adoption remains at a considerably earlier stage, with limited published, bank-level empirical evidence documenting actual implementation. Regional market analysis indicates that Zero-Trust adoption across emerging markets is concentrated primarily among financial institutions and telecommunications operators, with regional enterprises typically favouring phased rollouts that begin with identity and access management and multi-factor authentication before progressing to more advanced network-access and analytics capabilities[7]. This pattern is consistent with the broader observation in the banking-security literature that strong Identity and Access Management establishes the essential foundation of Zero-Trust, requiring banks to deploy robust systems capable of verifying the identity of every user and device before granting access to resources[4]. No Bank of Tanzania publication or comparable regional regulatory disclosure was identified that specifically documents Zero-Trust Architecture adoption, as distinct from general cybersecurity guidance, among supervised financial institutions, underscoring the scarcity of empirical, country-level evidence for East African banking markets relative to the global adoption data cited above.

Although information on the adoption of Zero-Trust Architecture among financial banks in Tanzania remains limited, National Microfinance Bank (NMB) is one bank that has adopted this technology strategy within its network to safeguard its cyberspace. This study is intended to provide empirical insight into the determinants of Zero-Trust Architecture adoption in commercial banks, using NMB Bank as its case study.

2.2 Theoretical Literature

Because this study investigates the acceptance and use of ZTA technology, together with the organizational-level variables associated with its adoption, individual-level theories such as the Technology Acceptance Model (TAM), the Unified Theory of Acceptance and Use of Technology (UTAUT), and Diffusion of Innovation (DOI) theory are not well suited as the primary lens for this study, since they were developed to explain individual rather than organizational adoption decisions. This study instead adopts the Technology–Organization–Environment (TOE) framework to explain ZTA adoption in commercial banks. The TOE framework holds that an organization's adoption of a technological innovation is shaped by three fundamental contextual factors: technology, organization, and environment[8]. The technological context encompasses both the internal and external technologies relevant to the organization—not only the specific innovation under consideration, but also the organization's existing technology infrastructure and the broader pool of available tools it could draw upon. The organizational context covers the internal characteristics and resources of the firm that shape its capacity to adopt and successfully implement an innovation. The environmental context covers external factors in the industry and institutional environment that create pressure toward or away from adoption, including the regulatory environment, industry pressure, and

customer pressure, among others.

2.3 Empirical Literature

2.3.1 Technology and Adoption of ZTA

Technological readiness is consistently identified as an important determinant of ZTA adoption in commercial banks. Deng and Inthiran[9], in a pilot investigation applying TOE-informed constructs to Zero-Trust Architecture adoption readiness among small and medium enterprises in the Asia-Pacific region, found that technological familiarity and readiness were significant factors shaping organizations' perceived need to adopt ZTA. In the Tanzanian context, Mwemezi and Mandari[10] examined big data analytics adoption using a TOE framework, drawing on 302 valid responses from top and middle managers across four leading Tanzanian commercial banks, and found that technological factors were significant predictors of adoption. Similarly, Kiyanga[11] examined cloud computing adoption at two top-ranked Tanzanian banks in Dar es Salaam, NMB and NBC, using a TOE framework focused specifically on technological factors, and found that security and privacy concerns were the most decisive technological determinants. By contrast, Nguyen, Le, and Vu[12], studying online retailing adoption among Vietnamese firms undergoing digital transformation, found that technological-context factors did not have a statistically significant effect on adoption. Technological readiness is therefore not a universally significant predictor across contexts, which motivates testing it directly within the Tanzanian banking sector. Accordingly, this study proposes:

H1: Technological readiness has a significant positive effect on ZTA adoption.

2.3.2 Organization and Adoption of ZTA

The organizational context encompasses the internal characteristics and resources of the firm that shape its capacity to adopt and successfully implement an innovation, including top management support, organizational structure, and internal resources such as financial capital, technical expertise, and human capital. Several studies, both globally and in Tanzania, have examined the organizational dimension of technology adoption. Nguyen, Le, and Vu[12], studying digital-transformation adoption among Vietnamese firms, found that organizational factors, particularly top management support, were significant predictors of adoption. In Tanzania, organizational influence has been examined in relation to other technologies but not explicitly in relation to ZTA (e.g., Mwemezi & Mandari[10]), leaving a gap for investigation of organizational determinants specific to ZTA adoption in commercial banks. This study therefore proposes:

H2: Organizational factors have a significant positive effect on ZTA adoption.

2.3.3 Environmental Factors and Adoption of ZTA

Environmental factors encompass regulatory bodies such as the Bank of Tanzania (BoT) and the Tanzania Communications Regulatory Authority (TCRA), as well as broader industry and customer pressure. Existing empirical studies, both globally and in the Tanzanian context, have rarely tested environmental factors directly and statistically as predictors of ZTA adoption. Pigola and Meirelles[13], for example, examined environmental and regulatory pressure only indirectly, treating it as operating through organizational governance rather than as a directly modelled predictor, drawing on qualitative interviews with 27 cybersecurity experts alongside their quantitative model. This leaves a research gap regarding the direct statistical testing of environmental factors in the Tanzanian banking context. Accordingly, this study hypothesizes:

H3: Environmental factors have a significant positive effect on ZTA adoption.

2.3.4 Employee Awareness and Adoption of ZTA

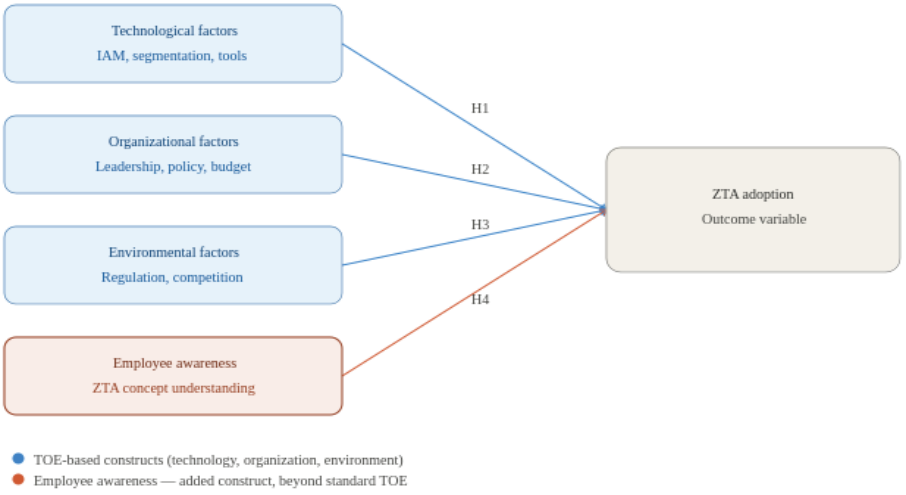
Deng and Inthiran[9] investigated employee awareness among small and medium businesses in the Asia-Pacific region, surveying 64 IT and security professionals about Zero-Trust Architecture. Their central finding was that the more familiar individuals were with what Zero-Trust actually entails, the more strongly they perceived their organization as needing it. Pigola and Meirelles[13], employing a mixed-methods design, similarly found that companies with a strong security culture were better positioned to adopt ZTA. In Tanzania, Lyimo and Shaaban[14] conducted a study at NMB Bank's Magomeni branch involving 50 employees and identified two central problems: first, that most employees believed cyber threats originated primarily from outside the bank, such as from hackers and scammers; and second, that non-technical staff regarded cybersecurity as "not their job." The study recommended that future interventions focus on training and improved security habits rather than on technology alone. This study therefore proposes:

H4: Employee awareness and understanding have a significant positive effect on ZTA adoption.

2.4 Research Gaps

The literature reviewed above indicates that, theoretically, technological, organizational, and environmental factors are expected to influence ZTA adoption, yet this expectation has not been empirically tested within Tanzanian commercial banks. Furthermore, while the TOE framework is conventionally applied with the organization as the unit of analysis, this study extends the framework by adding employee awareness as a fourth construct, thereby also incorporating the individual employee as a unit of analysis. This extension distinguishes the present study from prior TOE-based research and constitutes its principal theoretical contribution.

Figure 1: Conceptual Research Framework



3. Methodology

3.1 Research Design

This study employed a quantitative, cross-sectional research design, conducted in May 2025, to assess the factors influencing the adoption of Zero-Trust Architecture (ZTA) within NMB Bank PLC.

3.2 Research Area

The study was conducted at NMB Bank PLC headquarters in Dar es Salaam, Tanzania, the national hub for banking technology and cybersecurity operations. Focusing on the headquarters provided access to IT, cybersecurity, risk, and operations staff with direct experience of security architecture and access-control systems.

3.3 Population and Sampling

The target population consisted of 160 employees across IT and Security, Frontline Services, Risk and Compliance, and Middle/Senior Officer categories. The sample size was determined using the Yamane[15] formula:

$$n = N / (1 + N \cdot e^2)$$

With N = 160 and e = 0.05: $e^2 = 0.0025$; $N \cdot e^2 = 160 \times 0.0025 = 0.4$; $1 + N \cdot e^2 = 1.4$; $n = 160 / 1.4 = 114.3$. A sample size of 114 was therefore obtained at a 5% margin of error, representing a response rate of approximately 71.3% of the target population.

3.4 Sampling Technique

A stratified sampling technique was employed to ensure that every category of employee was represented in the study.

3.5 Ethical Considerations

Ethical approval was obtained prior to data collection. Participation was voluntary, and anonymity and confidentiality were guaranteed; no personal identifiers were collected. All sources used in the literature review were properly cited to avoid plagiarism.

4. Results, Discussion, and Implications

4.1 Demographic Characteristics of Respondents (N = 114)

Table 1: Demographic characteristics of respondents

Demographic Variable	Category	Frequency	Percentage
Gender	Male	80	70%
	Female	34	30%
Education Level	Degree	80	70%
	Master's	23	20%
	Diploma	11	10%
Age Group	20–30	57	50%
	31–40	34	30%
	41–50	12	10%
	Above 50	11	10%
Total		114	100%

Of the 114 NMB employees who participated in this study, the majority were male, accounting for 70% (n = 80) of the sample, while female respondents made up 30% (n = 34). In terms of educational attainment, most respondents held a bachelor's degree (70%, n = 80), followed by those with a master's degree (20%, n = 23) and diploma holders (10%, n = 11), indicating a generally well-educated workforce. Regarding age distribution, half of the respondents (50%, n = 57) were between 20 and 30 years old, followed by 30% (n = 34) aged between 31 and 40 years, while those aged 41 to 50 and above 50 each accounted for 10% (n = 12 and n = 11, respectively). This demographic profile suggests that the sample was predominantly composed of young, educated, male employees, which is relevant to interpreting the study's findings within the context of NMB's workforce composition.

4.2 Data Analysis Techniques

Quantitative data were analyzed using SPSS (Version 20). Techniques included: (i) descriptive statistics (means and standard deviations); (ii) Cronbach's alpha for reliability; (iii) assumption testing (linearity, normality, homoscedasticity, multicollinearity, and independence of errors); (iv) Pearson correlation analysis; and (v) multiple linear regression to determine the predictors of ZTA adoption.

All regression assumptions were met: residuals were normally distributed (Shapiro–Wilk p = .611); no autocorrelation was present (Durbin–Watson = 2.250); variance inflation factor (VIF) values below 2 indicated no multicollinearity; and scatterplots confirmed linearity and homoscedasticity.

4.2.1 Validity and Reliability

Validity was assessed through expert review of the questionnaire items by three specialists—two cybersecurity experts and one methodology expert—an exercise that improved item clarity and alignment with the research constructs. Reliability, assessed using Cronbach's alpha, indicated acceptable internal consistency across all constructs.

Table 2: Summary of reliability of constructs

Construct	Cronbach's α	Reliability	Remarks
Technological Factors	.778	Acceptable	Indicates consistent measurement across items
Environmental Factors	.775	Acceptable	Indicates consistent measurement across items
Employee Awareness	.711	Acceptable	Meets the .70 threshold for internal consistency
Organizational Factors	.705	Acceptable	Just above the .70 threshold; consistency confirmed
ZTA Adoption	.712	Acceptable	Meets the .70 threshold for internal consistency

All five constructs exceeded the commonly used .70 threshold, indicating acceptable internal consistency across the measurement scale as a whole.

4.2.2 Regression Results

The regression analysis, carried out using SPSS, produced the results summarized in Table 3.

Table 3: Regression predictors summary

Predictor	Mean	Beta (β)	Sig. (p)	Interpretation
Employee Awareness	3.79	0.673	< .001	Strongest positive predictor
Technological Factors	3.57	0.224	.021	Moderate positive predictor
Organizational Factors	3.63	-0.136	.343	Not significant
Environmental Factors	3.84	-0.009	.964	Not significant

4.3 Discussion of Results

This study set out to investigate the adoption of Zero-Trust Architecture (ZTA), one of the modern technologies increasingly adopted by financial institutions in developing countries such as Tanzania. The study was operationalized through four hypotheses, as illustrated in Figure 1. The results indicated that two hypotheses were supported and statistically significant, while the remaining two were not.

H1: Technological readiness has a significant positive effect on ZTA adoption (supported: β = .224, p = .021). This confirms that technology, as expected, is a fundamental factor in the adoption of ZTA within financial institutions in the Tanzanian context. Although no prior studies on ZTA specifically were identified within Tanzanian financial institutions, studies on related technologies, such as cloud computing[11] and big data analytics[10], report similar findings. This consistency suggests that employees' acceptance of modern technologies in Tanzanian banks depends heavily on technological factors such as multi-factor authentication (MFA), single sign-on (SSO), and identity federation capability.

H2: Organizational factors have a significant positive effect on ZTA adoption (not supported: β = -.136, p = .343). This result contrasts with Nguyen, Le, and Vu's[12] finding that organizational factors, particularly top management support, significantly predicted technology adoption among Vietnamese firms, and with Mwemezi and Mandari's[10] findings on technology adoption in the Tanzanian banking sector. Two explanations are plausible. First, adoption at NMB may currently be driven more by technical necessity and individual practice—IT staff implementing controls because they are required to, and employees following procedures because they understand the associated risk—rather than by a coordinated, top-down organizational push. Second, NMB may have formal policies and leadership commitment recorded in governance documents that have not yet translated into the resourcing, training investment, or day-to-day reinforcement that employees would actually perceive and respond to. This latter explanation echoes Pigola and Meirelles'[13] finding that strategic commitment alone did not significantly predict actual ZTA implementation, whereas security culture and follow-through did.

H3: Environmental factors have a significant positive effect on ZTA adoption (not supported: β = -.009, p = .964). Several explanations may account for this result within the Tanzanian context. No Bank of Tanzania publication or regional regulatory disclosure was identified that specifically names ZTA as an expected or required security framework; where BoT cybersecurity guidance exists, it is likely framed at a general level (for example, data protection, IT governance, and incident reporting) rather than prescribing a specific architecture such as Zero-Trust. It is also possible that competitive or peer pressure remains minimal because ZTA adoption is not yet widespread among Tanzanian banks, leaving little external benchmark to generate adoption pressure.

H4: Employee awareness and understanding have a significant positive effect on ZTA adoption (supported: β = .673, p < .001). This finding aligns with a broader pattern emerging in the global ZTA literature[9] and indicates that ZTA adoption at NMB Bank is currently more a human-capital challenge than a technological or governance one. It also extends earlier findings by Lyimo and Shaaban[14] at NMB's Magomeni branch, who found that employees mistakenly believed threats originated primarily from outside the organization, and that non-technical staff regarded cybersecurity as outside their

responsibility; the present study's results suggest that these same awareness gaps continue to shape ZTA adoption outcomes at the institutional level.

4.4 Implications for Literature and Practitioners

These findings carry implications for both the academic literature and practitioners.

4.4.1 Implications for Literature (Theoretical Contribution)

First, this study extends TOE into an underexplored regional and technological context. Most TOE applications originate from developed-economy or general-technology settings, such as cloud computing, ERP, and e-commerce. This study is among the first to apply TOE specifically to Zero-Trust Architecture within a Sub-Saharan African banking context, extending the framework's empirical reach and testing whether its established patterns hold in a resource-constrained, legacy-system-heavy environment. The results show that TOE's relative construct weights are context-dependent rather than universal.

Second, the findings challenge the completeness of standard TOE for security-architecture adoption. This adds empirical weight to the argument, echoed in Pigola and Meirelles[13] and Deng and Inthiran[9], that pure TOE is insufficient for explaining the adoption of security technologies whose effectiveness depends on ongoing human behaviour rather than one-time organizational commitment, supporting the case for hybrid frameworks that augment TOE with individual-level constructs drawn from UTAUT or TAM.

Third, the study adds to the small but growing literature on cybersecurity technology adoption in emerging markets. Given the near-total absence of Tanzania-specific ZTA literature, this study establishes a reference point against which future researchers can compare findings, whether through replication at other Tanzanian or East African banks, or through longitudinal follow-up to examine whether the dominance of awareness persists as ZTA adoption matures locally.

4.4.2 Implications for Practitioners

For bank management at NMB and similarly positioned institutions, these findings suggest a need to redirect investment priorities. Since awareness outweighs both technological and organizational factors in predicting adoption, and since awareness and training interventions are typically far less capital-intensive than infrastructure overhauls, the practical implication is clear: awareness-building should be prioritized alongside, rather than after, technology procurement.

For IT and risk/security leadership, awareness gaps should be treated as an operational risk rather than merely a training checkbox. The dominance of awareness suggests that even well-provisioned ZTA infrastructure will underperform if staff do not understand or commit to it; security leaders should therefore build continuous, role-specific awareness reinforcement into the ZTA rollout plan as an integral component, not an afterthought.

For regulators, including the Bank of Tanzania and similar supervisory bodies, general cybersecurity guidance may not be sufficient to drive ZTA adoption specifically. If BoT and comparable regulators wish to accelerate ZTA adoption across the sector, this implies a need for more explicit, ZTA-specific regulatory expectations or guidance, rather than relying on general cybersecurity or data-protection rules to indirectly push banks toward Zero-Trust models.

For technology vendors and consultants serving this market, the findings suggest that bundling awareness and training components with technical implementation, rather than selling infrastructure alone, is more likely to match what actually drives client-side adoption success.

5. Conclusion, Recommendations, and Future Studies

5.1 Conclusion

This study set out to examine the determinants of Zero-Trust Architecture (ZTA) adoption within the Tanzanian banking sector, using NMB Bank PLC as a case study and grounding the investigation in an extended Technology–Organization–Environment (TOE) framework augmented with an employee awareness construct. Employing a quantitative, cross-sectional design, data were collected from 114 respondents and analyzed using multiple regression.

The results provide mixed support for the study's four hypotheses. Technological readiness was found to have a significant positive effect on ZTA adoption ($\beta = .224$, $p = .021$), confirming that infrastructure maturity—including identity and access management capability, network segmentation, and authentication tooling—remains a meaningful, if secondary, driver of adoption. Organizational factors ($\beta = -.136$, $p = .343$) and environmental/regulatory factors ($\beta = -.009$, $p = .964$) did not

emerge as statistically significant predictors, suggesting that, within this sample, leadership commitment, formal policy, and external regulatory or competitive pressure are not currently the primary forces shaping ZTA adoption decisions at the institution studied. By contrast, employee awareness and understanding of ZTA principles emerged as by far the strongest and most significant predictor of adoption ($\beta = .673$, $p < .001$), indicating that human factors—rather than technology procurement or institutional mandate—currently constitute the central determinant of Zero-Trust adoption at NMB Bank.

These findings suggest that ZTA adoption in this Tanzanian banking context is presently a human-capital challenge more than a technological or institutional one, and that the standard TOE framework, while partially applicable, is insufficient on its own to fully explain adoption outcomes for a security architecture whose effectiveness depends heavily on continuous, informed human behaviour.

5.2 Recommendations

First, for NMB and bank management, employee awareness and training programmes should be prioritized as the primary near-term investment, given that awareness emerged as the strongest predictor of ZTA adoption ($\beta = .673$, $p < .001$). Recommended actions include instituting mandatory, role-specific ZTA training modules for both technical and non-technical staff, delivered on a recurring basis (for example, quarterly) rather than as a one-off onboarding exercise, since continuous reinforcement is more likely to sustain the behavioural vigilance that ZTA depends on.

Second, for NMB and bank management, the specific misconception that cybersecurity is "IT's responsibility" should be addressed directly. Consistent with earlier institutional findings at NMB[14], training content should explicitly correct the tendency to view threats as externally sourced only, and should clarify that every employee, not only technical staff, plays a role in maintaining Zero-Trust principles such as least-privilege access and continuous verification.

Third, regulators should develop ZTA-specific regulatory guidance rather than relying solely on general cybersecurity or data-protection mandates.

Finally, other financial institutions operating in similar emerging-market contexts should not assume that leadership buy-in or regulatory and competitive pressure alone will drive ZTA adoption.

5.3 Future Studies

First, future research should replicate this study across multiple Tanzanian or East African banks to test whether the dominance of awareness over organizational and environmental factors holds more broadly, or whether it is specific to NMB Bank's institutional context.

Second, future research should employ longitudinal designs to establish whether awareness causally drives ZTA adoption, or whether the relationship runs partly in the reverse direction, with adoption exposure itself increasing awareness over time—a distinction that the current cross-sectional design cannot resolve.

Funding

No

Conflict of Interests

The authors declare that there is no conflict of interest regarding the publication of this paper.

Reference

[1] ORDR. (2026). Zero trust statistics 2026 report. https://ordr.net/blog/zero-trust-statistics-2026-report

[2] National Institute of Standards and Technology. (2020). Zero trust architecture (NIST Special Publication 800-207). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207

[3] Okta, Inc. (2026). State of zero trust security report. As cited in Swif (2026), Zero trust statistics for 2026: Adoption, ROI, federal mandates, and what comes next. https://www.swif.ai/blog/zero-trust-statistics

[4] BobsGuide. (2025). Implementing zero trust security frameworks in banking. https://www.bobsguide.com/implementing-zero-trust-security-frameworks-in-banking/

[5] IBM Security. (2025). Cost of a data breach report 2025. IBM Corporation.

[6] BlueRadius. (2026). Zero trust implementation strategies. https://blueradius.io/zero-trust-implementation-strategies

[7] DataM Intelligence. (2026). Zero trust security market size, share, trends & forecast (2026–2035). https://www.datamintelligence.com/research-report/zero-trust-security-market

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

[9] Deng, Y., & Inthiran, A. (2025). Towards zero trust architecture: A pilot study on information systems security readiness amongst small and medium enterprises [Completed research paper]. University of Canterbury, Department of Accounting and Information Systems.

[10] Mwemezi, J., & Mandari, H. (2024). Big data analytics usage in the banking industry in Tanzania: Does perceived risk play a moderating role on the technological factors? Journal of Electronic Business & Digital Economics, 3(3), 318–340. https://doi.org/10.1108/JEBDE-01-2024-0001

[11] Kiyanga, D. S. (2024). Factors influencing the adoption of cloud computing technology in the Tanzanian banking industry: A multifaceted analysis. The Journal of Informatics, 4(1). Institute of Accountancy Arusha.

[12] Nguyen, T. H., Le, X. C., & Vu, T. H. L. (2022). An extended technology-organization-environment (TOE) framework for online retailing utilization in digital transformation: Empirical evidence from Vietnam. Journal of Open Innovation: Technology, Market, and Complexity, 8(4), Article 200. https://doi.org/10.3390/joitmc8040200

[13] Pigola, A., & Meirelles, F. de S. (2025). Zero trust in practice: A mixed-methods study under the TOE framework. Journal of Cybersecurity and Privacy, 5(4), Article 99. https://doi.org/10.3390/jcp5040099

[14] Lyimo, B. J., & Shaaban, S. Y. (2021). Cybersecurity awareness among employees in banking industry in Tanzania: A case of National Microfinance Bank – Magomeni Branch. Olva Academy – School of Researchers, 3(1), 1–4.

[15] Yamane, T. (1967). Statistics: An introductory analysis (2nd ed.). Harper and Row.