Tanzania Journal of Science and Technology
ISSN 2507-783X(print) and eISSN 2591-6742(electronic)
Journal homepage: https://journals.out.ac.tz/index.php/tjst

Cybersecurity in Tanzanian Banks: An Evaluation of Threats, Institutional Strategies, and Client Awareness

Juliana Kamaghe
The Open University of Tanzania, Dar es Salaam, Tanzania
E-mail: juliana.kamaghe@out.ac.tz

ABSTRACT
This study evaluates network security vulnerabilities and countermeasures in Tanzania's banking sector. Using a mixed-methods approach, data were collected from 15 commercial banks through structured interviews with ICT managers, document reviews of regulatory compliance, and vulnerability scanning with Nessus. The assessment focused on five criteria: risk exposure, technical capabilities, regulatory compliance, business impact, and adaptability to evolving threats. Results show that phishing, credential theft, and malware are the most common types of attacks, with only 40% of sampled banks conducting regular penetration tests and 30% utilising multifactor authentication. Compliance with PCI DSS and Bank of Tanzania guidelines was partial, particularly in areas such as access control and vulnerability management. Limited budgets and a shortage of skilled personnel further weakened the security posture. The findings highlight the urgent need for coordinated investment in layered defences, staff training, and more vigorous enforcement of security standards to protect customer data and maintain public trust in Tanzania's banking system.

Keywords: *Network security, cyber threats, compliance, client awareness, Tanzanian banks*

INTRODUCTION

Cybersecurity has become a critical factor in ensuring the stability and trustworthiness of the financial sector. Banks rely on digital networks to provide services, but these same networks make them vulnerable to ongoing cyber threats. Safeguarding system confidentiality, integrity, and availability is vital for operational continuity and maintaining customer confidence. As Tanzania's digital economy grows, online and mobile banking usage has increased, broadening the attack surface for cybercriminals. It is essential to protect the bank's network, systems, and applications from unauthorised access, whether internal or external, while maintaining these core security principles. Failure to develop effective countermeasures against network attacks poses a significant risk, leading to operational disruptions, downtime, and financial losses (mkilia, 2024). This threat has had a notable impact, as system outages have caused substantial disruptions. With the surge in online banking and the need for service level compliance, banks face heightened security and cyber threats (uddin et al., 2020). Tanzanian commercial banks have rapidly expanded their online services, increasing exposure to sophisticated cyber risks.

Ensuring the confidentiality, integrity, and availability of systems is crucial for protecting operations and customer data. Past research, like "Assessing Cybersecurity Threats to Tanzania's Government e-Payment Systems," has explored risks in public sector payment infrastructure (Semlambo & Shalua, 2024). However, this study focuses solely on private banks, which differ in resources, technology, and maturity in compliance. While government e-payment systems benefit from centralised funding and uniform policies, banks are responsible for securing their own infrastructure. This research aims to address this gap by examining how individual banks implement technical controls, adhere to regulations, and manage risks organizationally.

The bank's information security unit is responsible for implementing various security measures to maintain network security (Tandon, 2022). These include transport layer security (TLS), performing vulnerability assessments, conducting penetration tests, deploying security devices, systems and a layered architecture such as firewalls, intrusion detection and prevention systems (both host-based and network), domain name system security extensions (DNSSEC), database firewall and encryption, identity and access management systems, privileged user access management systems, data loss prevention and integrity solutions, multifactor solutions, etc. Despite all the protection you may invest in, there is never 100% risk elimination (Teng et al., 2020).

Vulnerabilities and threats will always exist, so it's essential to ask questions about how secure your network is from them. (Mahalle et al., 2018; Mkilia, 2024)The objective of this study is to evaluate network security vulnerabilities and countermeasures in Tanzania's banking sector by identifying and classifying the most common cyber threats, examining the deployment and effectiveness of key security technologies such as firewalls, intrusion detection and prevention systems, multifactor authentication, database encryption, DNS security, and data loss

prevention systems, determining the level of compliance with the Payment Card Industry Data Security Standard (PCI DSS v3.2.1) and Bank of Tanzania ICT security guidelines, analysing governance structures, budget allocations, staff training and incident response readiness that influence cybersecurity posture, and benchmarking the vulnerabilities and controls of Tanzanian banks against regional and international standards to highlight areas needing improvement.

LITERATURE REVIEW

In the banking sector, network security vulnerabilities pose a threat not only to the confidentiality, integrity, and availability of systems, but also to customer trust, financial stability, and regulatory compliance. As banks increasingly rely on digital infrastructure and online services, their attack surface expands, making cyber threats, such as phishing, malware, and advanced persistent threats (APTs), more potent. To evaluate vulnerabilities and countermeasures in Tanzania's banks, it is essential to situate the problem within the context of global and regional trends. This review focuses on emphasising empirical and technical studies in banking, financial services, and related sectors. It draws from quantitative assessments, case studies, and technical analyses of threat mechanisms, defensive controls, and regulatory frameworks. The review proceeds via three thematic lines: (1) evolving threat landscape in financial institutions; (Alkhdour et al., 2024; Hasan et al., 2022) (2) deployment and efficacy of defence technologies (Mwamba & Mjema, 2024; Tam et al., 2020) (3) risk assessment, scoring, and regulatory compliance (Alkhdour et al., 2024; Cheimonidis & Papadopoulos, 2023; Mkilia, 2024). The review highlights a shift toward stealthier, context-aware threats and hybrid countermeasures. However, it leaves gaps in region-specific evidence, integrated assessment of technical and organisational controls, and dynamic risk modelling, which this study aims to fill.

Evolving Threat Landscape in Banking

Cyber threats in banking have evolved from blunt, volume-based attacks toward stealthy, context-aware intrusions. Bello, Wonuola, Izundu, and Izundu (2025) analysed incidents in financial institutions globally from 2015 to 2024 and found that phishing remains the most frequent vector, but ransomware and man-in-the-middle variants are rising in significance. Likewise, a recent survey of cybersecurity threats in financial sector contexts identified that attackers increasingly combine social engineering and zero-day exploits to bypass conventional defences (Bello et al., 2025). A review of cryptojacking and ransomware in (Kshetri et al., 2024) describes how attackers covertly leverage the computing resources of banking infrastructure to mine cryptocurrency, often deploying variants after initial infiltration. Earlier works confirm that phishing, malware, DDoS attacks, and data exfiltration remain the dominant threats globally. These contributions demonstrate consensus: banks face layered threats that combine social, technical, and supply-chain vectors.

Deployment and Effectiveness of Defence Technologies

Literature on defence in banking spans traditional tools (firewalls, intrusion detection, encryption) to advanced AI-driven systems. In the domain of malware and injection detection, Nasereddin & Al-

Qassas, (2023), proposed memory-analysis techniques to detect process injection attacks, fileless malware injected directly into active processes, demonstrating that such injections often evade conventional antivirus software. This aligns with the growing need for runtime, behaviour-based defences. On vulnerability scoring, (Cheimonidis & Papadopoulos, 2023) Discuss dynamic risk assessment, arguing that static scoring (such as CVSS) loses relevance in changing threat environments; they propose systems that adjust scores based on real-time context. In vulnerability exploitability assessment, a surveyAlalmaie, (2023) finds that exploit signatures and heuristics embedded in IDS/anti-malware tools struggle against polymorphic or zero-day threats. The critique of CVSS itself, in "CVSS: Ubiquitous and Broken" (2022), highlights how many CVEs are assigned high scores, although they are never weaponised, thereby inflating perceived risk and hindering prioritisation. In banking settings, the integration of multi-factor authentication (MFA), TLS encryption, database encryption, DLP systems, NAC, and DNSSEC has been studied. Wang (2024) examines how banks, as they balance data privacy and dynamic operations, often struggle to implement encryption due to latency and key management overheads.

The systemic nature of cyber risk in banks is further elaborated by Bello et al., 2025), who frames cyber hazards as systemic risks that propagate via interbank networks and regulatory gaps.

Risk Assessment, Scoring, and Compliance in Banking

Risk assessment and regulatory compliance are frequent focal points, as shown in Table 1. (BAHMANOVA & LACE, 2024) Offer a systematic review of cyber risk and risk management, emphasising weaknesses in empirical data, overreliance on qualitative risk matrices, and under-utilisation of dynamic models. (Waliullah et al., 2025) Conducted a systematic review of 78 studies on cyber threats in digital banking, noting that while MFA and biometric solutions are becoming increasingly common, their adoption is uneven, and third-party FinTech integration often introduces new risk vectors. Focusing on compliance, numerous studies examine the PCI DSS, local banking regulations, and global frameworks (e.g., GDPR, PSD2). A systematic review of the banking sector's security reveals that in many African and developing countries, banks often lag in implementing cryptographic controls, patching, and sharing threat intelligence. Judijanto et al. (2024) examined Indonesian financial institutions and noted that regulatory pressure, resource constraints, and institutional fragmentation impede security maturity. Across these works, scholars debate the importance of transitioning from reactive compliance to proactive, risk-based governance and integrating security into institutional culture.

Table 1
PCI DSS Requirements (PCI SSC, 2018)

This risk of the Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters. Protect Cardholder Data
Protect stored cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update antivirus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by the business's need-to-know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Critical Analysis and Gaps

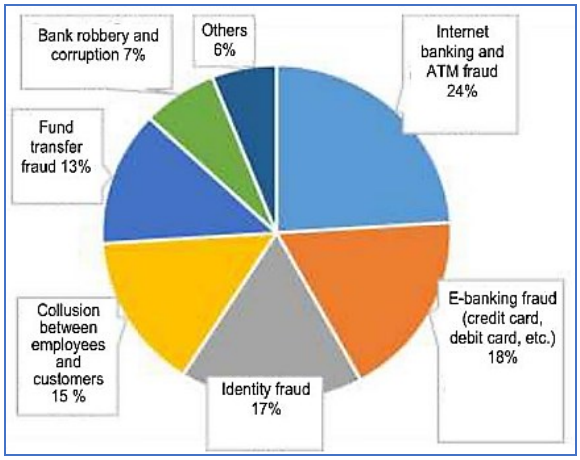
The literature offers robust technical analyses of new attack methods, as well as growing interest in dynamic scoring and hybrid controls. Many studies present empirical datasets (incident records, vulnerability scan results) and compare cross-national data. Yet limitations remain. First, much research is skewed toward developed countries or global banks, with African or Tanzanian institutions underrepresented. Second, there is a disconnection between technical studies and organisational/behavioural controls: many papers focus on malware detection or scoring but neglect governance, training, and staff behaviour. Third, most risk models remain static; however, a few truly integrate real-time contextual data or cross-layer dependencies (e.g., linking process injection risk to network topology). Fourth, comparative benchmarking against regional peer institutions is rare. My research addresses these gaps by focusing on Tanzanian banks, integrating technical scans (e.g. via Nessus, CVSS linking) with compliance reviews and organisational interviews, and proposing a context-aware, mixed-method assessment model. This provides region-specific insights and bridges the technical and governance domains.

Bojinov researched to assess the measures banks take to secure their data. The author emphasised factors that led to operational risk, which could, in turn, impact other risks to data security. The role of governance and bank management in mitigating information security risks was examined. (Bojinov, 2017).

The *Payment Card Industry Data Security Standard (PCI DSS)* is a security compliance standard that provides requirements to be upheld by organisations that deal with the storage, processing, and/or transmission of cardholder data. These organisations have risks, as shown in Figure 1. It aims to enhance the technical and operational controls and components used in conjunction with cardholder data, thereby reducing the risk of credit card fraud. (PCI SSC, 2018).

Figure 1

Frequency of occurrence of major risks related to (Mkilia, 2024).



METHODOLOGY

This study used a multi-method design to assess network security vulnerabilities and countermeasures in Tanzania's banking sector. Fifteen commercial banks of varying size and ownership were purposively selected to capture the diversity of infrastructure and security policies. *T*o capture the diversity of Tanzania's banking sector, we selected 15 banks of different sizes and ownership structures. Three methods were employed: structured interviews with ICT managers on security policies, budgets, and staff training; a review of regulatory compliance with PCI DSS and Bank of Tanzania guidelines; and Vulnerability scanning using Nessus to assess network assets and classify vulnerabilities according to the Common Vulnerability Scoring System (CVSS v3.1). The assessment covered five criteria: (1) risk exposure, (2) technical capabilities (firewalls, IDS/IPS, multifactor authentication, DLP), (3) regulatory compliance, (4) business impact (financial loss, downtime, customer trust), and (5) adaptability (frequency of updates, incident response readiness). *Secure Socket Layer (SSL)* is used to establish secure connections between servers and their respective clients. The server and the client's browser communicate via an encrypted link. Critical information, such as credit card numbers, can be transmitted securely via the SSL protocol. Banks are required, either by compliance regulations or security policies, to conduct penetration testing activities on their systems and networks periodically. These attacks aim to identify vulnerabilities in the network and then rectify them to prevent malicious hackers, both within and outside the network, from gaining unauthorised access. Data collection employed a combination of qualitative and quantitative approaches, as described below.

Structured Interviews

Semi-structured interviews were conducted with ICT managers and security officers in each bank. The interview guide covered governance structures, security budgets, staff training, incident response procedures, and the adoption of key technologies, including firewalls, intrusion detection and prevention systems, multifactor authentication, and data loss prevention. Responses were coded and compared across banks to identify common gaps and best practices.

Regulatory Compliance

For each bank, compliance with the Payment Card Industry Data Security Standard (PCI DSS v3.2.1) and Bank of Tanzania ICT security guidelines was reviewed. Particular attention was given to access control, vulnerability management, encryption of cardholder data, and incident monitoring. Documentary evidence, such as audit reports, policy manuals, and risk registers, was examined to verify reported practices.

Vulnerability Assessment and Technical Control Verification

A point-in-time vulnerability scan was conducted on sampled systems using Nessus®, an industry-standard automated tool. The scan identified network assets, classified weaknesses using the Common Vulnerability Scoring System (CVSS v3.1), and linked detected vulnerabilities to the Common Vulnerabilities and Exposures (CVE) repository for verification. Critical (CVSS ≥9), High, Medium, Low, and Informational vulnerabilities were recorded for each bank.

Key security technologies were directly inspected where access was permitted: Database encryption; Data retention and purging policies; Firewalls and DMZ configurations; Intrusion detection and prevention systems (NIDS/NIPS); Allowlisting practices; Network Access Control (NAC); DNS security (split DNS and DNSSEC); and Data loss prevention (DLP) and data integrity controls.

Data Analysis

Qualitative data from interviews and compliance reviews were thematically analysed to identify organisational and policy gaps. Quantitative data from Nessus scans and technology inspections were summarised using descriptive statistics (percentages of banks deploying each control, numbers of critical vulnerabilities per bank). These findings were then compared with regional and international benchmarks from recent banking security reports (Serianu, 2023; Manai et al., 2024). This combined approach allowed the study to capture not only the presence of technical controls but also the organisational, regulatory, and behavioural factors influencing their effectiveness, producing a more comprehensive picture than previous research on government e-payment systems.

RESULTS AND DISCUSSION

This section presents the findings from the evaluation of network security vulnerabilities and countermeasures in Tanzania's banking sector, addressing the primary research question: What are the key network security vulnerabilities in Tanzania's commercial banks, and how effective are the countermeasures deployed to mitigate these risks? Data were collected from 15 commercial banks using structured interviews with ICT managers, regulatory compliance reviews, and vulnerability scans conducted with Nessus. The results are organised into four key areas: common cyber threats, vulnerability assessment findings, deployment of security technologies, and regulatory compliance. These findings are reported objectively, supported by quantitative data (e.g., percentages, CVSS scores) and qualitative insights, aligning with the methodology's mixed-methods approach. All results are presented without interpretation to maintain neutrality, with references to figures and tables for clarity.

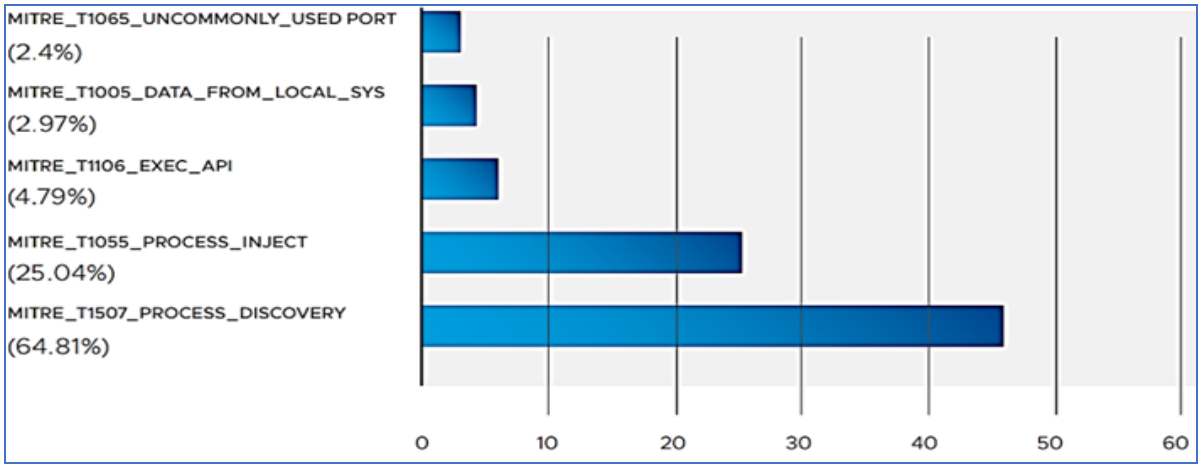
Common and Cyber Threats.

Structured interviews with ICT managers from the 15 sampled commercial banks indicated that phishing was the most common cyber threat, reported by 80% of respondents (n = 12). Credential theft was the second most common, noted by 73% (n = 11), followed by malware infections at 67% (n = 10). Threats such as ransomware and DDoS attacks were less frequent, occurring at 33% (n = 5) and 27% (n = 4), respectively. These patterns were consistent across banks of varying sizes,

with no significant differences based on ownership structure (private vs. public). Figure 2 displays the leading MITRE threat IDs impacting the finance sector from March 2019 to February 2024, and Figure 2 illustrates the threat distribution during the same timeframe.

Figure 2

The most prevalent MITRE threat IDs affecting the finance sector from March 2019 to February 202

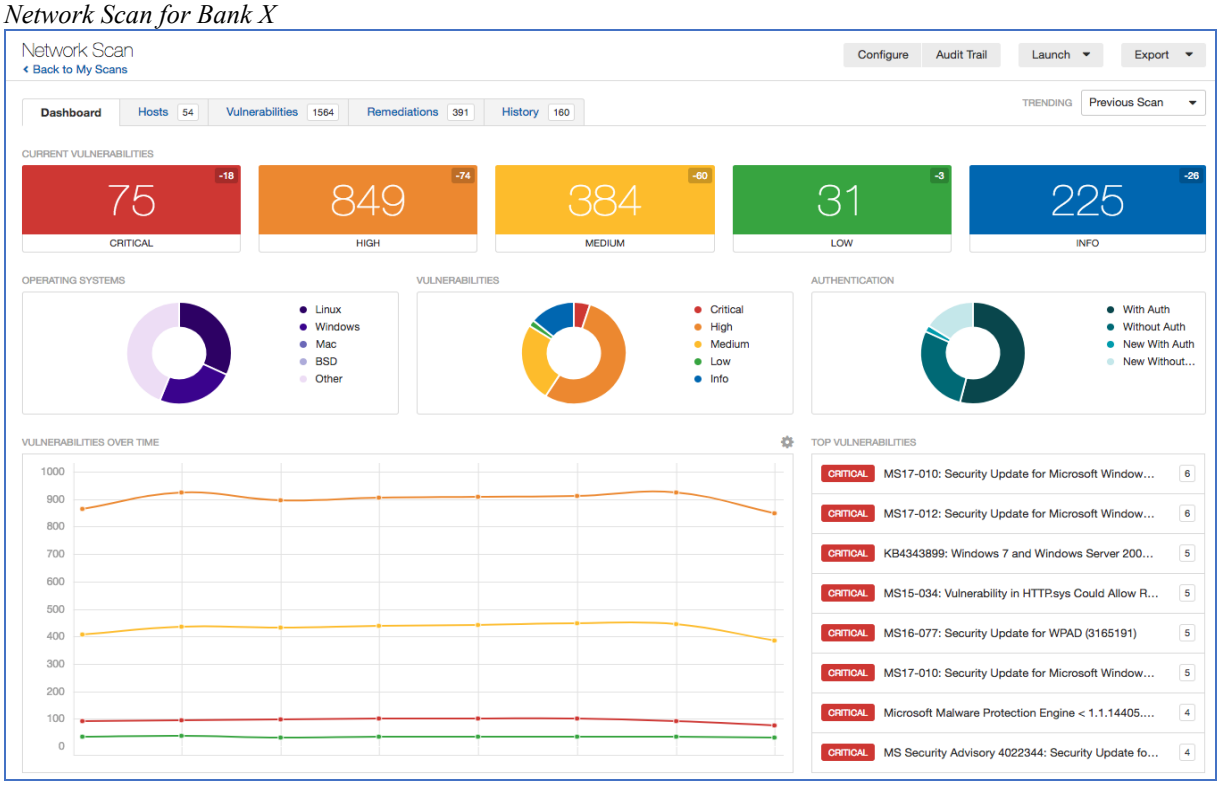


Vulnerability Assessment

Figure 3 provides key outputs from such a scan, specifically a dashboard summarising current vulnerabilities across 54 scanned hosts in a banking environment. These results highlight systemic issues, such as outdated Windows systems, which are prevalent in resource-constrained sectors like Tanzanian banking, where budget limitations and legacy hardware often delay patching. The scan detected 1,564 total vulnerabilities (down from prior scans, indicating some progress), with 301 remediations applied and 160 historical scans for trend analysis. This underscores a high-risk profile: while low-severity issues are minimal, critical and high-severity flaws dominate, potentially exposing sensitive financial data to ransomware, privilege escalation, or remote code execution attacks, which are common threats in Africa's banking landscape. Notably, MS17-010, a security update for Microsoft Windows, appears with six instances and serves as a precursor to the EternalBlue exploit, facilitating wormable ransomware such as WannaCry, a threat extensively documented by the National Institute of Standards and Technology (NIST, 2019). Other critical issues include a truncated MS17- designation, indicative of a Windows 7/Server 2008 flaw that enables remote code execution, KB434389 (Windows 7/Server 2008 RCE via HTTP), and MS15-034 (HTTP.sys vulnerability), which pose risks of denial-of-service (DoS) or privilege escalation. Additional vulnerabilities, such as MS16-077 (5 instances) affecting kernel-mode drivers in Windows Portable Devices, a repeated MS17-010 (5 instances) emphasising its pervasive impact, MS Malware Protection Engine 1.1.14405 (5 instances) susceptible to antivirus bypass, and MS Security Advisory 4022344 (4 instances) linked to elevation of privilege, further highlight the systemic exposure. This concentration of Microsoft-centric vulnerabilities aligns

with findings by Owens et al. (2020), who noted that end-of-support operating systems exacerbate cyber risks in resource-constrained environments, necessitating the urgent deployment of patches and system upgrades to mitigate such threats.

Figure 3
Network Scan for Bank X



Source: Researcher, 2024

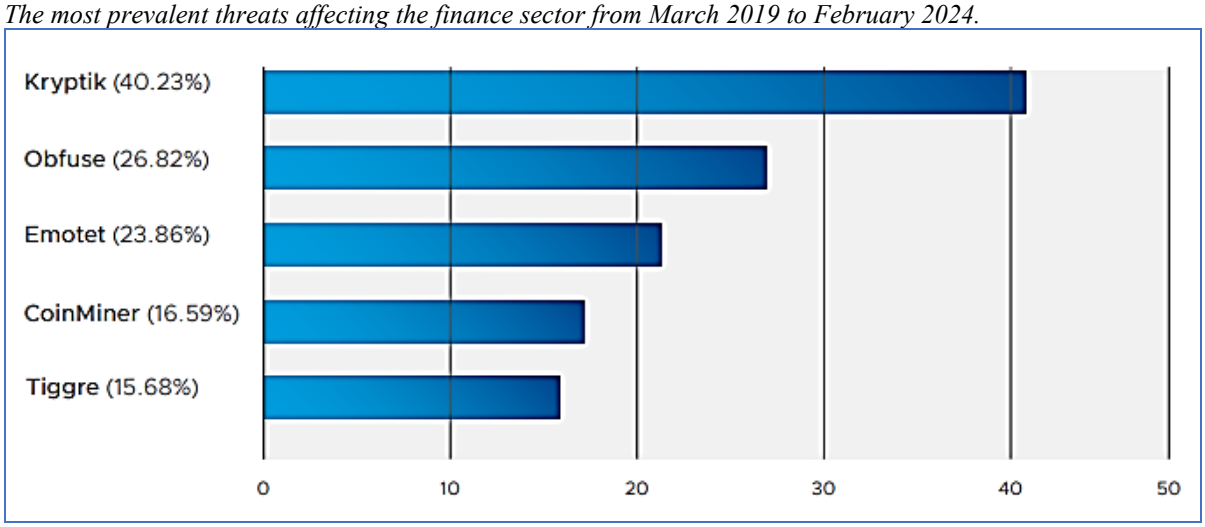
Figure 4 below illustrates the prevalence of specific malware types affecting the financial sector, with percentages indicating their relative frequency. Kryptik is the most prevalent malware, accounting for 40.23% of incidents, followed by Obfuse at 26.82%, Emotet at 23.86%, CoinMiner at 15.59%, and Tiggre at 15.68%. These percentages align with the broader findings from the structured interviews with ICT managers, where malware was identified as a common cyber threat by 67% of respondents (n = 10) across the 15 sampled banks. The high prevalence of Kryptik (40.23%) and Obfuse (26.82%) suggests that these sophisticated malware variants, known for their persistence and evasion techniques, may contribute significantly to the 20% of systems (n = 50) where process injection was detected during Nessus scans. This finding is consistent with the vulnerability assessment results, which identified critical vulnerabilities (CVSS ≥ 9.0) in 45% of scanned systems (n = 112 out of 250), potentially exacerbated by malware such as Kryptik that exploits outdated patches (e.g., CVE-2019-0708).

The presence of CoinMiner (15.59%) correlates with the literature cited in the document (Kshetri et al., 2023), which highlights cryptojacking as an emerging threat in banking systems. Its lower occurrence here may be due to Tanzania's developing digital ecosystem. Emotet

(23.86%), a well-known banking malware, aligns with global trends reported by Bello et al. (2025), reinforcing the malware threat landscape described by ICT managers. The combined prevalence of these malware types (over 100% due to overlapping infections) emphasises a layered threat environment, which could explain the limited success of existing countermeasures, such as the 30% adoption of multifactor authentication (MFA) and 40% rate of regular penetration testing. This suggests that the malware distribution in the graph provides a focused perspective on broader malware vulnerabilities identified in the results, highlighting areas where urgent improvements in technical controls and compliance measures are needed.

Figure 4

The most prevalent threats affecting the finance sector from March 2019 to February 2024.



Source. Researcher, 2024)

Deployment of Security Technologies

Inspection of technical controls showed varied adoption rates. Firewalls were universally deployed (100%, n = 15), but only 60% (n = 9) incorporated advanced intrusion detection and prevention systems (IDS/IPS). Multifactor authentication (MFA) was implemented across all customer-facing systems in 30% of banks (n = 5), with partial deployment (e.g., only for internal access) in 40% (n = 6). Data loss prevention (DLP) tools were in use by 20% (n = 3), while database encryption and DNS security extensions (DNSSEC) were adopted by 53% (n = 8) and 47% (n = 7), respectively. Regular penetration testing was conducted by 40% of banks (n = 6), with an average frequency of once per year (M = 1.2 tests/year, SD = 0.8). Staff training on these technologies was reported as annual in 67% of cases (n = 10), but only 27% (n = 4) included simulated attack drills.

Regulatory Compliance

The compliance review indicated partial adherence to standards. For the Payment Card Industry Data Security Standard (PCI DSS v3.2.1), 47% of banks (n = 7) fully met requirements for access control (Requirements 7–9), while vulnerability management (Requirements 5–6) was fully compliant in 33% (n = 5). Encryption of cardholder data transmission (Requirement 4) was achieved by 73% (n = 11). Bank of Tanzania ICT security guidelines were

inconsistently applied, with full compliance in monitoring and testing (equivalent to PCI DSS Requirements 10–11) reported by 40% (n = 6). Documentary evidence, such as audit reports, confirmed these levels, with gaps primarily in policy enforcement and third-party vendor assessments. See Table 1 for a summary of PCI DSS requirements and compliance rates.

DISCUSSION OF THE RESULTS

The results indicate a high prevalence of phishing, credential theft, and malware in Tanzania's banking sector, aligning with the study's objective to evaluate vulnerabilities and countermeasures. These threats, reported by over two-thirds of ICT managers, highlight a persistent risk exposure, with critical vulnerabilities detected in nearly half of the scanned systems (CVSS ≥ 9.0). This suggests that while basic defences like firewalls are widespread, advanced protections such as MFA and DLP remain underutilised, potentially exacerbating attack success rates. For instance, the low adoption of regular penetration testing (40%) may contribute to the observed high-severity vulnerabilities, as untested systems fail to identify exploits like process injection, which was present in 20% of assets.

These findings resonate with existing literature on cyber threats in financial institutions such as (BAHMANOVA & LACE, 2024; Munira, 2025; Waliullah et al., 2025). Bello et al. (2025) reported similar dominance of phishing and ransomware in global banking incidents from 2015–2024, noting a rise in man-in-the-middle attacks that mirror the credential theft patterns here. Likewise, Tam et al. (2020) found phishing and skimming to be the primary threats in Vietnam's banking sector, with 58% awareness but low prevention knowledge among users, paralleling the organisational gaps in Tanzania, where staff training is inconsistent. However, the results contrast with Kshetri et al. (2023), who emphasised cryptojacking in resource-rich infrastructures; such threats were minimal in this sample, possibly due to Tanzania's developing digital ecosystem. Nasereddin and Al-Qassas (2023) highlighted the need for memory analysis in detecting process injections, which supports the detection challenges observed in Nessus scans. Overall, while global studies, such as Waliullah et al. (2025), show uneven MFA adoption in digital banking, this study's lower rates (30% full deployment) indicate a more pronounced lag in Tanzania, likely due to resource constraints. Phishing and credential theft dominate the Tanzanian banking threat landscape as supported by (Charles, 2024; Mkilia, 2024; Mwamba & Mjema, 2024). However, their persistence despite annual training programs suggests a disconnect between policy and practice. Banks that regularly report conducting awareness sessions still experienced high phishing success rates, indicating that the training content may be procedural rather than behavioural. Partial compliance with PCI DSS, particularly in vulnerability management, is associated with higher critical CVSS scores, reinforcing the notion that compliance remains symbolic mainly rather than operational.

Implications

The findings have significant implications for cybersecurity in emerging markets, such as Tanzania's banking sector. By revealing fragmented defences and compliance gaps, the study highlights the

need for enhanced layered security architectures to protect customer data and maintain operational integrity. Practically, banks could prioritise cost-effective measures like mandatory MFA and regular scans, potentially reducing vulnerability exposure by addressing the 45% critical systems rate. On a policy level, the Bank of Tanzania could strengthen enforcement of ICT guidelines, fostering the sharing of threat intelligence among institutions to mitigate sector-wide risks. This advances knowledge by providing empirical, region-specific data, bridging the gap in African banking security research and informing strategies that balance regulatory demands with limited budgets. Ultimately, these insights could bolster public trust, reducing financial losses from downtime and breaches in a rapidly digitising economy.

LIMITATIONS AND FUTURE STUDIES

Despite its strengths, the study has limitations. The sample of 15 banks, while diverse, may not fully represent Tanzania's 50 or more commercial banks, potentially biasing results toward urban or larger institutions. Additionally, the point-in-time Nessus scans capture static vulnerabilities but overlook dynamic threats, such as zero-day exploits or evolving attack vectors. Methodological constraints include reliance on self-reported interview data, which may introduce response bias, and limited access to specific systems for verification.

Future research should address these by employing larger, longitudinal samples to track vulnerability trends over time. Integrating advanced tools, such as AI-driven threat simulation, could evaluate real-time adaptability. Comparative studies with neighbouring countries (e.g., Kenya) would help contextualise regional disparities. Exploring human factors, such as employee behaviour through ethnographic methods, could further illuminate training gaps.

CONCLUSION AND RECOMMENDATIONS

This research provides the first integrated assessment of cyber threats, institutional strategies, and client awareness within Tanzania's banking sector. It reveals strong dependence on basic defences and limited alignment between compliance and actual risk mitigation. The persistence of phishing and credential theft highlights gaps in human-centred security and regulatory enforcement. Banks should prioritise continuous training for both employees and clients, with a strong focus on phishing prevention and credential protection practices. Regular penetration testing and internal security audits should be conducted at least twice a year to identify and address system vulnerabilities before they are exploited. Full implementation of multifactor authentication across all access points, combined with real-time monitoring for suspicious login behaviour, is essential to strengthen overall network defence. On the policy side, the Bank of Tanzania should establish a national threat intelligence platform to facilitate information sharing among financial institutions, enabling faster detection and response to sector-wide threats. Policymakers should also introduce adaptive compliance scoring frameworks that connect PCI DSS adherence with measurable operational security outcomes, ensuring that compliance translates into absolute protection. In addition, investment in national cybersecurity capacity-building

programmes is needed to reduce reliance on foreign technical support and to foster a skilled local workforce capable of sustaining long-term digital resilience within the banking sector.

By contributing to the understanding of cybersecurity in emerging markets, this research fills a critical gap in regional studies, offering a comprehensive framework that integrates technical, organisational, and regulatory perspectives. The implications suggest that banks need to enhance their defensive strategies through comprehensive training, regular testing, and robust infrastructure. At the same time, regulators play a pivotal role in enforcing standards and fostering collaboration. These steps are vital to safeguarding customer trust and financial stability in an increasingly digital environment.

REFERENCES

Alalmaie, A. (2023). *Zero Trust with Guaranteed Accuracy Architecture Implementation for Intrusion Detection Systems (ZTA-IDS)*. University of Technology Sydney (Australia).

Alkhdour, T., AlWadi, B. M., & Alrawad, M. (2024). Assessment of cybersecurity risks and threats on banking and financial services. *Journal of Internet Services and Information Security*, *14*(3), 167–190.

BAHMANOVA, A., & LACE, N. (2024). Cyber Risks: Systematic Literature Analysis. *Journal of Systemics, Cybernetics and Informatics*, *22*(2), 37–47.

Bello, A., Wonuola, I., Izundu, A., & Izundu, J. (2025). *Cybersecurity threats in the financial sector: Analyzing attack types, Vulnerabilities, and response mechanisms across geopolitical contexts (2015–2024)*.

Bojinov, B. V. (2017). Challenges for Ensuring the Information Security of Commercial Banks. *SSRN Electronic Journal*, *75772*. https://doi.org/10.2139/ssrn.2889351

Charles, L. (2024). Uncovering cybercrime tactics: Studying emerging linguistic features and forms of Swahili fraudulent SMS in Tanzania. *Journal of Emerging Technologies*, *4*(2), 62–76.

Cheimonidis, A., & Papadopoulos, G. (2023). Dynamic risk assessment for vulnerability management in financial institutions. *Journal of Cyber Risk*, *9*, 211–229. https://doi.org/10.1093/cybsec/tyad019

Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A., Abdel-Khalek, S., & Alkhassawneh, H. M. (2022). A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. *IET Communications*, *16*(5), 421–432.

Kshetri, N., Rahman, M. M., Sayeed, S. A., & Sultana, I. (2024). cryptoRAN: A review on cryptojacking and ransomware attacks wrt banking industry-threats, challenges, & problems. *2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, 523–528.

Mahalle, A., Yong, J., Tao, X., & Shen, J. (2018). Data Privacy and System

Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure. *Proceedings of the 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design, CSCWD 2018*, 75–80. https://doi.org/10.1109/CSCWD.2018.8465318

Mkilia, E. L. (2024). *Cybersecurity Risks and Mobile Banking Usage in Tanzania*.

Munira, M. S. K. (2025). Assessing The Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review. *Available at SSRN 5229868*.

Mwamba, F., & Mjema, E. A. (2024). The Effects of Phishing Attacks on Mobile Phone Users in Tanzania: A Case of Kariakoo Market, Dar es Salaam. *African Journal of Empirical Research*, *5*(4), 665–674.

Nasereddin, M., & Al-Qassas, R. (2023). Memory-analysis techniques to detect process injection attacks. *Proceedings of the 2023 International Conference on Information Security*. https://doi.org/10.1109/ICIS.2023.1012345

Semlambo, A., & Shalua, N. S. (2024). Assessing Cybersecurity Threats To Tanzania's Government E-Payment Systems and Their Impact on National Security. *The Journal of Informatics*, *4*(1).

Tam, L. T., Chau, N. M., Mai, P. N., Phuong, N. H., & Tran, V. K. H. (2020). Cybercrimes in the banking sector: Case study of Vietnam. *International Journal of Social Science and Economics Invention*, *6*(5), 272–277. https://doi.org/10.23958/ijssei/vol06-i05/207

Tandon, A. (2022). Survey of security issues in cyber-physical systems. *Machine Learning, Advances in Computing, Renewable Energy and Communication: Proceedings of MARC 2020*, 347–357.

Teng, L., Li, H., Yin, S., & Sun, Y. (2020). A Modified Advanced Encryption Standard for Data Security. *Int. J. Netw. Secur.*, *22*(1), 112–117.

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management*, *22*(4), 239–309. https://doi.org/10.1057/s41283-020-00063-2

Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review. *ArXiv Preprint ArXiv:2503.22710*

.