Cybersecurity Strategies as Enablers of Digital Transformation in Commercial Banks: Evidence from Zimbabwe

Collade N. Murungu[1], Morelate Kupfuwa[2], Majory Nyazema[3]

[1]Collade Murungu, Midlands State University, Harare, Zimbabwe

[2]Morelate Kupfuwa, Midlands State University, Harare, Zimbabwe

[3]Majory Nyazema, Midlands State University, Harare, Zimbabwe

DOI: https://doi.org/10.47772/IJRISS.2026.10200321

Received: 28 January 2026; Accepted: 03 February 2026; Published: 09 March 2026

ABSTRACT

The rapid adoption of digital technologies in the banking sector has transformed service delivery, operational efficiency, and customer engagement. However, this transformation has simultaneously exposed commercial banks to escalating cybersecurity threats, particularly in developing economies. This study examines the effectiveness of cybersecurity strategies in promoting digital transformation within commercial banks in Zimbabwe. Anchored in the Technology Acceptance Theory, Routine Activity Theory, and Fraud Triangle Theory, the study adopts a positivist research philosophy and a quantitative explanatory design. Data were collected using structured questionnaires administered to employees and customers of five major Zimbabwean commercial banks. Statistical analysis was conducted using SPSS, employing descriptive statistics, correlation analysis, and regression modeling. The findings reveal uneven adoption of digital transformation initiatives, with significant gaps in service automation and data analytics capabilities. Cybersecurity challenges, including skills shortages, cultural resistance, and legacy systems, were identified as major constraints. Empirical results demonstrate a strong positive relationship between cybersecurity strategies and digital transformation, with cybersecurity explaining approximately 68% of the variance in digital transformation outcomes. The study concludes that robust cybersecurity measures are not merely protective mechanisms but critical enablers of successful digital transformation in the banking sector. It recommends targeted investment in cybersecurity infrastructure, continuous workforce upskilling, and stronger regulatory frameworks to enhance secure digital innovation. The study contributes to the limited empirical literature on cybersecurity and digital transformation in emerging market banking contexts.

Keywords: Cybersecurity; Digital transformation

INTRODUCTION

The global banking sector is undergoing rapid digital transformation driven by advances in financial technologies, changing customer expectations, and the need for greater operational efficiency. Digital banking platforms, mobile applications, data analytics, and automated service delivery systems have become central to modern banking operations. In Zimbabwe, commercial banks have increasingly adopted digital channels to improve financial inclusion, reduce transaction costs, and enhance customer convenience. However, the expansion of digital banking has simultaneously increased banks' exposure to cyber threats such as card cloning, phishing, ransomware attacks, and data breaches, which undermine customer trust and threaten financial stability. As digital transformation deepens, cybersecurity has emerged as a critical concern, particularly in developing economies where regulatory frameworks, technical infrastructure, and cybersecurity skills remain underdeveloped (Muteba, 2020; Muganyi, 2022; Reserve Bank of Zimbabwe, 2021)

Existing literature acknowledges that cybersecurity is essential for safeguarding digital banking systems, yet many studies treat cybersecurity primarily as a technical or defensive function rather than a strategic enabler of digital transformation. Prior studies in both developed and developing contexts emphasize the role of firewalls, encryption, and authentication mechanisms in reducing cybercrime (Alabi, 2019; Mhlanga, 2020). Theoretical

perspectives such as the Technology Acceptance Theory, Routine Activity Theory, and Fraud Triangle Theory further suggest that technology adoption, motivated offenders, and organizational vulnerabilities interact to shape cybersecurity outcomes. However, empirical research linking cybersecurity strategies directly to the success of digital transformation initiatives—especially within African banking systems—remains limited. Most available studies focus on individual technologies or isolated cyber risks, offering insufficient insight into how comprehensive cybersecurity strategies influence broader digital transformation outcomes in commercial banks

This gap is particularly pronounced in the Zimbabwean context, where the banking sector has rapidly digitized despite persistent cybersecurity incidents and skills shortages. While reports indicate that a substantial proportion of banking transactions in Zimbabwe are conducted digitally, cybercrime continues to escalate due to legacy systems, inadequate regulatory enforcement, and limited cybersecurity expertise (ZICT Report, 2020; Mpofu & Bello, 2021). Existing local studies largely examine digital banking adoption or cybercrime trends independently, with little empirical evidence assessing whether cybersecurity strategies actively promote or constrain digital transformation. Consequently, there is limited understanding of how cybersecurity investments, governance structures, and human capital development shape the effectiveness of digital transformation in Zimbabwe's commercial banks. This study addresses this literature gap by empirically examining the relationship between cybersecurity strategies and digital transformation outcomes within the sector

The importance of this research lies in its practical, theoretical, and policy relevance. For commercial banks, the findings provide evidence-based insights into how cybersecurity can be leveraged not only to mitigate risk but also to accelerate secure digital innovation. For regulators and policymakers, the study offers guidance on strengthening cybersecurity frameworks to support sustainable digital banking growth. From a theoretical perspective, the research extends existing models of technology adoption and cybercrime by contextualizing them within an emerging-market banking environment. By empirically demonstrating cybersecurity's role as a driver of digital transformation, this study contributes to the limited body of African-focused banking literature and supports informed decision-making as Zimbabwe's financial sector continues its transition toward a digitally driven economy

Main Objective

To empirically examine the effect of cybersecurity strategies on digital transformation in commercial banks in Zimbabwe.

METHODOLOGY SUMMARY

This study adopted a positivist research philosophy, which is appropriate for examining relationships between variables through objective measurement and statistical analysis. A quantitative explanatory research design was employed to assess the effect of cybersecurity strategies on digital transformation in commercial banks in Zimbabwe. This design enabled the study to test hypothesised relationships and establish the strength and direction of associations between cybersecurity measures and digital transformation outcomes

The target population comprised employees and customers of selected commercial banks operating in Zimbabwe, specifically Stanbic Bank, ZB Bank, CBZ Bank, BancABC, and Nedbank Zimbabwe. These banks were selected based on their market presence, level of digital transformation, and exposure to cybersecurity incidents. A probability sampling technique was used to ensure representativeness and reduce sampling bias. Primary data were collected using structured questionnaires, which were designed to capture information on digital transformation initiatives, cybersecurity strategies, and perceived challenges affecting implementation

The questionnaire items were measured using Likert-scale instruments, allowing for quantitative assessment of respondents' perceptions. Prior to analysis, the reliability of the research instrument was tested using Cronbach's alpha, confirming acceptable internal consistency. Data analysis was conducted using SPSS version 29.0, employing descriptive statistics to summarize respondent characteristics and the extent of digital transformation adoption. Inferential analysis included Spearman's correlation to assess the relationship between cybersecurity strategies and digital transformation, as well as regression analysis to determine the

predictive power of cybersecurity measures on digital transformation outcomes Ethical considerations were observed throughout the study, including voluntary participation, confidentiality, and informed consent. The methodological approach ensured validity, reliability, and objectivity, enabling robust empirical evaluation of cybersecurity as a strategic enabler of digital transformation within Zimbabwe's commercial banking sector

RESEARCH FINDINGS

Response Rate and Data Reliability

The study achieved a satisfactory response rate, indicating adequate participation from both employees and customers of the selected commercial banks. Reliability analysis of the survey instrument produced acceptable Cronbach's alpha coefficients, confirming internal consistency across the constructs measuring digital transformation, cybersecurity strategies, and implementation challenges. This reliability justified the use of inferential statistical techniques for hypothesis testing and model estimation

Extent of Digital Transformation Adoption

Findings revealed that digital transformation adoption among Zimbabwean commercial banks is uneven across functional areas. Digital channels such as mobile banking, internet banking, ATMs, and cardless transactions were moderately implemented, reflecting banks' efforts to enhance customer convenience and transaction efficiency. However, more advanced aspects of digital transformation showed significant weaknesses. Service automation recorded relatively low mean scores, particularly in automated account maintenance and customer analytics, indicating limited integration of intelligent systems in core banking operations. Similarly, the adoption of data analytics and artificial intelligence remained underdeveloped, suggesting that banks are still at an early stage of leveraging digital technologies for strategic decision-making and personalized service delivery

Challenges Affecting Digital Transformation

The study identified several critical challenges constraining effective digital transformation. Skills shortages emerged as the most severe challenge, with respondents indicating insufficient availability of cybersecurity and digital technology expertise within banks. Cultural resistance to change also ranked highly, reflecting organizational reluctance to move away from traditional banking processes. Additional constraints included legacy systems, inadequate financial resources, and regulatory uncertainties. These challenges collectively limit banks' capacity to deploy secure and scalable digital solutions, increasing their vulnerability to cyber threats and operational inefficiencies

Cybersecurity Strategies Implemented by Banks

Analysis of cybersecurity strategies showed that banks have implemented basic security measures such as authentication controls, transaction monitoring, and fraud prevention mechanisms. However, advanced cybersecurity capabilities—such as real-time threat intelligence, behavioral analytics, and comprehensive incident response frameworks—were not uniformly adopted across institutions. Employee cybersecurity awareness and training programs were inconsistently applied, further exposing banks to human-related cyber risks. Despite these limitations, respondents generally acknowledged cybersecurity as a critical requirement for sustaining digital banking services

Relationship Between Cybersecurity and Digital Transformation

Correlation analysis revealed a strong positive relationship between cybersecurity strategies and digital transformation, with a Spearman correlation coefficient of approximately $\boldsymbol{\rho = 0.82}$, indicating a high degree of association. Regression analysis further confirmed that cybersecurity strategies significantly predict digital transformation outcomes. The model showed that cybersecurity strategies explain about 68% of the variation in digital transformation levels ($\boldsymbol{R^2 = 0.68}$). The regression coefficient indicated that a one-unit improvement in cybersecurity strategies leads to an estimated 0.86-unit increase in digital transformation performance. These

results provide strong empirical support for the alternative hypothesis that cybersecurity strategies significantly promote digital transformation in commercial banks in Zimbabwe

CONCLUSIONS

Based on the empirical findings, the study concludes that cybersecurity strategies are a critical enabler of digital transformation rather than merely a defensive function within Zimbabwean commercial banks. While banks have made progress in adopting basic digital channels, the full benefits of digital transformation remain constrained by weak service automation, limited use of advanced analytics, and insufficient cybersecurity capabilities. The strong positive relationship between cybersecurity and digital transformation demonstrates that banks cannot successfully digitize operations without simultaneously strengthening their cybersecurity posture.

The study further concludes that human and organizational factors—particularly skills shortages and cultural resistance—pose greater barriers to digital transformation than technology alone. Even where digital infrastructure exists, inadequate cybersecurity training and governance structures undermine effective implementation. These findings reinforce theoretical perspectives from the Technology Acceptance Theory and Routine Activity Theory, which emphasize the importance of trust, user capability, and guardianship in technology adoption and crime prevention.

Overall, the study establishes that strengthening cybersecurity strategies enhances customer confidence, operational resilience, and the sustainability of digital banking initiatives. For Zimbabwe's banking sector, effective digital transformation requires integrated investment in cybersecurity infrastructure, human capital development, and regulatory support. Failure to align digital innovation with robust cybersecurity frameworks risks undermining financial stability and eroding public trust in digital banking systems.

REFERENCES

1. African Cybersecurity Report (2022) Cybercrime in Africa: A Growing Concern. African Cybersecurity Alliance.
2. Alabi, O.A. (2019) 'Cybersecurity threats to financial institutions: A review', Journal of Financial Crime, 26(4), pp. 1042-1056.
3. Alaeddini, M., Salehi, M. and Razavi, S.M. (2019) 'Digital transformation in banking: A systematic literature review', Journal of Business Research, 100, pp. 203-226.
4. Albrecht, W.S., Albrecht, C.O., and Albrecht, C. (2021) 'Fraud Detection Using the Fraud Triangle Theory and Data Mining', Journal of Financial Crime, 28(4), pp. 1043-1057. DOI: https://doi.org/10.1108/JFC-09-2020-0136.
5. Alhassan, I., et al. (2020) 'Customer engagement in banking: The role of cybersecurity', Journal of Financial Services Marketing, 25(3), pp. 245-258.
6. Al-Hawari, M.A., Al-Natour, M. and Al-Madi, F. (2025) 'Understanding mobile banking adoption via the technology acceptance model: evidence from Jordan', Banks and Bank Systems, 20(1), pp. 23-37. DOI: http://dx.doi.org/10.21511/bbs.20(1).2025.03.
7. American Bankers Association (2023) 'Preferred Banking Methods: Survey Results'. Available at: https://www.aba.com (Accessed: 25 January 2025).
8. Azeus Convene (2024) 'Digital Transformation in Banking: Key Drivers'. Available at: https://www.azeusconvene.com/articles/digital-transformation-in-banking (Accessed: 25 January 2025).
9. Bada, A. & Sasse, A. (2015) 'The Challenges of Legacy Systems in Banking', Journal of Financial Services Technology, 11(2), pp. 78-89.
10. Balnaves, M. (2020) Introduction to quantitative research methods: An investigative approach. 2nd edn. London: Sage Publications.
Creswell, J.W., Creswell, J.D. and Guetterman, T.C. (2018) Research design: Qualitative, quantitative, and mixed methods approaches. 5th edn. Thousand Oaks: Sage Publications.
Polit, D.F. and Beck, C.T. (2017) Nursing research: Generating and assessing evidence for nursing practice. 10th edn. Philadelphia: Lippincott Williams & Wilkins.

11. Begg, D. (2024) 'Importance of Digital Forensics Process Models: Some Examples', Forensics Weekly Executive Summaries. Available at: https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summaries/importance-of-digital-forensics-process-models-some-examples/ (Accessed: 3 February 2025).
12. Berman, S.J., 2012. Digital transformation: Opportunities to create new business models. Strategy & Leadership, 40(2), pp.16-24. https://doi.org/10.1108/10878571211209314
13. Binariks (2024) 'Emerging Trends in Digital Banking to Dominate in 2025'. Available at: https://binariks.com/blog/digital-banking-trends/ (Accessed: 25 January 2025).
14. Bryman, A. (2016) Social research methods. 5th edn. Oxford: Oxford University Press. Comte, A. (1853) The positive philosophy of Auguste Comte. London: John Chapman. Creswell, J.W. (2014) Research design: Qualitative, quantitative, and mixed methods approaches. 4th edn. Thousand Oaks: Sage Publications. Giddens, A., Duneier, M., Appelbaum, R.P. and Carr, D. (2017) Introduction to sociology. 11th edn. New York: W.W. Norton & Company.
15. Bryman, A. (2016) Social research methods. 5th edn. Oxford: Oxford University Press. Creswell, J.W. and Creswell, J.D. (2018) Research design: Qualitative, quantitative, and mixed methods approaches. 5th edn. Thousand Oaks: Sage Publications. Robson, C. and McCartan, K. (2016) Real world research. 4th edn. Chichester: Wiley.
16. Bryman, A. (2016) Social research methods. 5th edn. Oxford: Oxford University Press. Hürlimann, M. (2019) Explanatory research: Methods and applications. Berlin: Springer.
17. Bryman, A. and Bell, E. (2019) Business research methods. 5th edn. Oxford: Oxford University Press.
18. Bryman, A. and Bell, E. (2019) Business research methods. 5th edn. Oxford: Oxford University Press.
19. Bryman, A. and Bell, E. (2022) Business Research Methods. 5th edn. Oxford: Oxford University Press.
20. CardPro Ltd (2020) Card Cloning and Fraud in Zimbabwe.
21. CardPro Ltd (2020) Card Cloning and Fraud in Zimbabwe. CardPro Ltd.
22. Chikafu, E. & Mlambo, C., 2022. Application of descriptive statistics in social science research: A Zimbabwean perspective. Zimbabwe Journal of Research, 10(3), pp. 77-89.
23. Chikoko, L. (2023) 'The rise of fintech in Zimbabwe: Implications for traditional banks', The Financial Gazette, 18 July, p. 8. KPMG (2022) Global banking outlook: Meeting the demands of the digital customer. New York: KPMG Publications.
24. Chikomba, L. (2021) Cyber and Data Protection Act: Implications for Zimbabwean Businesses. Harare: Legal Publishers. Reserve Bank of Zimbabwe (2022) Annual Report on Cybersecurity in the Banking Sector. Harare: RBZ Publications.
25. Chikwata, T. (2020) Cybersecurity technologies in Zimbabwe's banking sector: A technical perspective. Harare: Tech Publishers. Dube, S. (2021) 'Digital transformation and cybersecurity in Zimbabwe: Bridging the research gap', Journal of African Finance and Technology, 7(2), pp. 45–60. Muriu, J. (2017) Cybersecurity in Zimbabwe's banking sector: A case study of cardholder fraud. Harare: University of Zimbabwe Press. Reserve Bank of Zimbabwe (2023) Cybersecurity and digital transformation in Zimbabwe's financial sector: Challenges and opportunities. Harare: RBZ Publications.
26. Chikwata, T. (2021) Digital banking in Zimbabwe: Trends and challenges. Harare: Tech Publishers. Dube, S. (2021) 'Digital transformation in Zimbabwe's banking sector: Opportunities and barriers', Journal of African Finance and Technology, 7(3), pp. 34–48. Mashiri, T. (2022) 'Cardless withdrawals: A game-changer for Zimbabwean banks', TechZim, 10 June. Available at: www.techzim.co.zw (Accessed: 20 October 2023). Reserve Bank of Zimbabwe (2023) Digital transformation in Zimbabwe's banking sector: Trends and challenges. Harare: RBZ Publications.
27. Chikwata, T. (2021) Digital banking in Zimbabwe: Trends and challenges. Harare: Tech Publishers. Mashiri, T. (2022) 'Automation in Zimbabwe's banking sector: Opportunities and challenges', TechZim, 15 July. Available at: www.techzim.co.zw (Accessed: 20 October 2023).

Reserve Bank of Zimbabwe (2023) Digital transformation in Zimbabwe's banking sector: Trends and challenges. Harare: RBZ Publications.

28. Chikwata, T. (2021) Digital banking in Zimbabwe: Trends and challenges. Harare: Tech Publishers. Mashiri, T. (2022) 'The rise of digital payments in Zimbabwe', TechZim, 30 October. Available at: www.techzim.co.zw (Accessed: 20 October 2023).
Old Mutual Zimbabwe (2022) Omari: Revolutionizing mobile money in Zimbabwe. Harare: Old Mutual Publications.
Reserve Bank of Zimbabwe (2023) Digital transformation in Zimbabwe's banking sector: Trends and challenges. Harare: RBZ Publications.
29. Chikwata, T. (2023) 'Funding digital transformation in Zimbabwe's banking sector', The Herald, 22 January, p. 9.
Reserve Bank of Zimbabwe (2022) Economic and digital transformation outlook for the banking sector. Harare: RBZ Publications.
30. Chimucheka, T. and Mandipaka, F. (2015) 'Cybersecurity frameworks: A study on Zimbabwean financial institutions', Journal of Financial Services Management, 19(1), pp. 12-25.
31. Chitungo, S.K. and Munongo, S., 2019. Blockchain technology adoption in Zimbabwean banks: Opportunities and challenges. Journal of Innovation and Business Best Practices, 2019, pp.1-12. https://doi.org/10.5171/2019.123456
32. Chou, D.C., et al. (2021) 'Cybersecurity investment: A pathway to innovation', International Journal of Information Management, 57, pp. 102-110.
33. Cloudficient (2024) The Stages of EDRM. Available at: https://www.cloudficient.com/blog/the-stages-of-edrm (Accessed: 3 February 2025).
34. Cloward, R.A. and Ohlin, L.E. (1960) Delinquency and Opportunity: A Theory of Delinquent Gangs. Glencoe: Free Press.
35. Creswell, J.W. and Creswell, J.D. (2018) Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 5th edn. Thousand Oaks, CA: SAGE Publications.
36. Davis, F.D. (2023) 'Perceived usefulness, perceived ease of use, and user acceptance of information technology', MIS Quarterly, 47(1), pp. 319-340.
37. Davis, F.D. (2023) 'Perceived usefulness, perceived ease of use, and user acceptance of information technology', MIS Quarterly, 47(1), pp. 319-340.
38. DCM (2024) 'Top 5 Challenges in Digital Transformation for Banking'. Available at: https://dashdevs.com/blog/5-challenges-of-digital-transformation-in-banking/ [Accessed: 5 February 2025].
39. Deloitte (2022) AI and machine learning in fraud detection: A game-changer for banks. New York: Deloitte Publications.
KPMG (2021) Predictive analytics in banking: Transforming fraud detection. London: KPMG Publications.
Reserve Bank of Zimbabwe (2023) Guidelines on advanced fraud detection systems for commercial banks. Harare: RBZ Publications.
40. Deloitte (2022) Big data analytics in banking: Transforming fraud detection and prevention. New York: Deloitte Publications.
KPMG (2021) The role of big data in combating financial crime. London: KPMG Publications.
Reserve Bank of Zimbabwe (2023) Guidelines on leveraging big data analytics for cybersecurity. Harare: RBZ Publications.
41. Deloitte (2022) Collaborative cybersecurity: Strengthening the financial sector. New York: Deloitte Publications.
KPMG (2021) Industry partnerships in cybersecurity: A path to resilience. London: KPMG Publications.
Reserve Bank of Zimbabwe (2023) Guidelines on collaboration for cybersecurity in the banking sector. Harare: RBZ Publications.
42. Deloitte (2022) Identity and access management: A key pillar of cybersecurity. New York: Deloitte Publications.
KPMG (2021) Zero-trust security models: Transforming cybersecurity in banking. London: KPMG Publications.

Reserve Bank of Zimbabwe (2023) Guidelines on identity and access management for commercial banks. Harare: RBZ Publications.

43. Deloitte (2022) Real-time monitoring in banking: A cybersecurity imperative. New York: Deloitte Publications.
KPMG (2021) The role of SIEM systems in combating cyber threats. London: KPMG Publications.
Reserve Bank of Zimbabwe (2023) Guidelines on real-time monitoring and incident response for commercial banks. Harare: RBZ Publications.
44. DFRWS (2023) 'Forensic Challenges'. Available at: https://dfrws.org/forensic-challenges/ (Accessed: 3 February 2025).
45. Dillman, D.A., Smyth, J.D. and Christian, L.M. (2014) Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method. 4th edn. Hoboken, NJ: Wiley.
46. DiMaggio, P.J. and Powell, W.W. (1983) 'The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields', American Sociological Review, 48(2), pp. 147-160.
47. Dube, S. (2021) 'Digital literacy gaps in Zimbabwe's banking sector', The Sunday Mail, 14 March, p. 12.
McKinsey & Company (2020) Unlocking success in digital transformations. New York: McKinsey Publications.
48. Duc, J., Jabangwe, J., Paul, S. and Abrahamsson, P. (2024) 'Cybersecurity Concerns in Digital Banking: An Analysis', Journal of Financial Services Technology, 15(1), pp. 34-50.
49. Duc, J., Jabangwe, J., Paul, S. and Abrahamsson, P. (2024) 'Cybersecurity Concerns in Digital Banking: An Analysis', Journal of Financial Services Technology, 15(1), pp. 34-50.
50. Duc, J., Jabangwe, J., Paul, S. and Abrahamsson, P. (2024) 'Cybersecurity Concerns in Digital Banking: An Analysis', Journal of Financial Services Technology, 15(1), pp. 34-50.
51. Duc, J., Jabangwe, J., Paul, S., and Abrahamsson, P. (2017) 'Cybersecurity Concerns in Digital Banking: An Analysis', Journal of Financial Services Technology, 15(1), pp. 34-50.
52. EDRM.net (2023) EDRM Stages Standards. Available at: https://edrm.net/resources/frameworks-and-standards/edrm-model/edrm-stages-standards/ (Accessed: 3 February 2025).
53. Encyclopedia.com (2024) 'Differential Opportunity Structure'. Available at: https://www.encyclopedia.com/social-sciences/dictionaries-thesauruses-pictures-and-press-releases/differential-opportunity-structure (Accessed: 31 January 2025).
54. eSecurity Planet (2024) 'Cyber Security in Banking: Threats, Solutions & Best Practices'. Available at: https://www.esecurityplanet.com/cloud/cyber-security-in-banking/ (Accessed: 29 January 2025).
55. Eyer.ai (2024) 'Big data and cyber security: Bridging the gap'. Available at: https://eyer.ai/blog/big-data-and-cyber-security-bridging-the-gap/ (Accessed: 15 January 2025).
56. Fares, A., Butt, I., and Lee, J. (2023) 'The Influence of Institutional Factors on AI Adoption in EU Banking Cybersecurity', Journal of Financial Services Research. Available at: http://www.diva-portal.org/smash/get/diva2:1875709/FULLTEXT01.pdf (Accessed: 29 January 2025).
57. Financial Fraud Action Africa (2022) Cybercrime in Africa: A Growing Threat.
58. Financial Fraud Action Africa (2022) Cybercrime in Africa: A Growing Threat. Financial Fraud Action Africa.
59. Finn, J. and Downie, R. (2024) 'Navigating Digital Transformation in Banking with Cloud Computing', International Journal of Financial Services, 12(1), pp. 45-60.
60. Forbes (2023) 'The multidimensional relationship between AI and cybersecurity and its impact on fintech'. Available at: https://www.forbes.com/councils/forbestechcouncil/2023/06/08/the-multidimensional-relationship-between-ai-and-cybersecurity-and-its-impact-on-fintech/ (Accessed: 15 January 2025).
61. Fowler, F.J. (2014) Survey Research Methods. 5th edn. Thousand Oaks, CA: SAGE Publications.
62. Gibson Dunn (2024) The E-Discovery Life Cycle. Available at: https://www.gibsondunn.com/wp-content/uploads/documents/publications/E-DiscoveryBasics2-E-DiscoveryLifeCycle.pdf (Accessed: 3 February 2025).
63. Huang, J., Zhang, Y., & Chen, L. (2020) 'Modernizing Legacy Systems in Banking: Challenges and Strategies', International Journal of Information Management, 50(1), pp. 123-134.
64. Johnson, L. (2021) Harnessing secondary data for contemporary research: A comprehensive approach. 3rd edn. Chicago: Research Publications.

65. JPMorgan Chase and Co. (2020) Annual Report 2020. Available at: https://www.jpmorganchase.com/investor-relations/annual-reports (Accessed: 16 January 2025).
66. Kane, G.C., Palmer, D., Phillips, A.N., Kiron, D. and Buckley, N., 2015. Strategy, not technology, drives digital transformation. MIT Sloan Management Review, 14(1), pp.1-25.
67. Kaspersky (2018) Cybercrime in Africa: A Growing Concern.
68. Kaspersky (2018) Cybercrime in Africa: A Growing Concern. Kaspersky Lab.
69. Kassem, R. and Higson, A.W. (2022) 'The Evolution of Fraud Theory: From Cressey's Triangle to Contemporary Applications', International Journal of Law and Management, 64(2), pp. 321-335.
70. Kassem, R. and Higson, A.W. (2022) 'The Evolution of Fraud Theory: From Cressey's Triangle to Contemporary Applications', International Journal of Law and Management, 64(2), pp. 321-335.
71. Kaufmann, T., Graf, C. and Hinz, O. (2020) 'The impact of digital transformation on the banking industry', Journal of Business Economics, 90(3), pp. 281-307.
72. Khumalo, T. & Ndlovu, P., 2023. Digital banking adoption and customer experience in Zimbabwean financial institutions. Journal of African Business, 24(2), pp. 134-150.
73. Klimenko, A. (2023) 'Digital Transformation in Banking: A Systematic Review', Journal of Banking Innovation, 15(2), pp. 101-120.
74. Kohn, R. (2017) 'A Survey and Critique of Digital Forensic Investigative Models', International Journal of Computer Applications, 164(10), pp. 1-6. DOI: https://doi.org/10.5120/ijca2017914751.
75. KPMG (2021) 'Cybersecurity: Protecting your business'. Available at: https://home.kpmg/xx/en/home/insights/2021/01/cybersecurity.html (Accessed: 16 January 2025).
76. Kvale, S. and Brinkmann, S. (2015) InterViews: Learning the Craft of Qualitative Research Interviewing. 3rd edn. Thousand Oaks, CA: SAGE Publications.
77. Lawton, A. and Stacey, K. (2014) 'eDiscovery: The Process of Identifying and AnalyzingElectronic Data', International Journal of Digital Evidence, 13(1), pp. 1-15.
78. Leukfeldt, R. and Yar, M. (2024) 'A Review on the Application of Lifestyle-Routine Activity Theory in Cyber Criminology', Journal of Criminology and Forensic Studies, 6(1), pp. 180077. DOI: https://doi.org/10.1007/s10940-022-09564-7.
79. Liquid Technologies (2024) 'Zimbabwe's perceptions about cyber security need to change'. Available at: https://liquid.tech/zimbabwes-perceptions-about-cyber-security-need-to-change/ (Accessed: 16 January 2025).
80. Lyman, J. (2023) 'Technology Acceptance Theory: A Guide for Banking Institutions', Journal of Financial Services Research, 58(2), pp. 145-158.
81. Lyman, J. (2023) 'Technology Acceptance Theory: A Guide for Banking Institutions', Journal of Financial Services Research, 58(2), pp. 145-158.
82. Mago, S. and Chitokwindo, S., 2014. The impact of mobile money on financial inclusion in Zimbabwe: A case of EcoCash. Journal of Economics and Behavioral Studies, 6(10), pp.766-774.
83. Mago, S., 2018. Challenges of digital transformation in Zimbabwean banks: A case of selected commercial banks. Journal of African Business, 19(3), pp.466-480. https://doi.org/10.1080/15228916.2017.1416214
84. Mangayarkarasi, S. and Manikandan, R. (2022) 'Challenges in cybersecurity for banking sector', Journal of Financial Services Management, 26(2), pp. 45-60.
85. Mangudhla, T. (2021) 'Zimbabwe's brain drain: impact on the financial sector', Business Weekly, 15 March, p. 7.
PwC (2020) Global financial services talent trends. New York: PwC Publications.
86. Marelli, M. (2020) 'Challenges in Implementing eDiscovery in Digital Transformation', Journal of Digital Compliance, 5(2), pp. 45-58.
87. Marelli, M. (2020) 'Challenges in Implementing eDiscovery in Digital Transformation', Journal of Digital Compliance, 5(2), pp. 45-58.
88. Mashiri, T. (2022) 'Cybersecurity awareness in Zimbabwe's banking sector: Challenges and opportunities', TechZim, 8 September. Available at: www.techzim.co.zw (Accessed: 20 October 2023).
PwC (2021) Building a cybersecurity-aware workforce: Best practices for financial institutions. New York: PwC Publications.
Reserve Bank of Zimbabwe (2023) Guidelines on cybersecurity training and awareness for commercial banks. Harare: RBZ Publications.

89. Masuda, T., Shirasaka, K., Yamamoto, Y. and Hardjono, T. (2023) 'Understanding Spear-Phishing Attacks: Strategies and Countermeasures', International Journal of Cybersecurity Research, 9(2), pp. 78-92.
90. Masuda, T., Shirasaka, K., Yamamoto, Y. and Hardjono, T. (2023) 'Understanding Spear-Phishing Attacks: Strategies and Countermeasures', International Journal of Cybersecurity Research, 9(2), pp. 78-92.
91. Mhlanga, D. (2020) 'Cybersecurity awareness among bank employees in Zimbabwe', Journal of Cybersecurity, 6(1), pp. 1-12.
92. Mhlanga, D. (2020) 'Cybersecurity awareness among bank employees in Zimbabwe', Journal of Cybersecurity, 6(1), pp. 1-12.
93. Mhlanga, D. (2020) 'Cybersecurity awareness among bank employees in Zimbabwe', Journal of Cybersecurity, 6(1), pp. 1-12. doi: 10.1093/cybsec/tyaa001
94. MISA Zimbabwe (2021) 'Analysis of the Data Protection Act'. Available at: https://zimbabwe.misa.org/2021/12/06/analysis-of-the-data-protection-act/ (Accessed: 29 January 2025).
95. Mokhtar, M.B., Al-Hawari, M.A., Al-Natour, M., and Al-Madi, F. (2024) 'Mobile banking adoption—extending technology acceptance model with transaction convenience and perceived risk: A conceptual framework', International Journal of Financial Studies, 11(1), pp. 1-15.
96. Mokhtar, M.B., Al-Hawari, M.A., Al-Natour, M., and Al-Madi, F. (2024) 'Mobile banking adoption—extending technology acceptance model with transaction convenience and perceived risk: A conceptual framework', International Journal of Financial Studies, 11(1), pp. 1-15.
97. Mollah, M. A., Hassan, M. K. and Islam, M. S. (2020) 'Digital transformation in banking: A study on customer perception', Journal of Business and Economic Development, 5(1), pp. 1-13.
98. Mollah, M.A., Hassan, M.K. and Islam, M.S. (2020) 'Digital transformation in banking: A study on customer perception', Journal of Business and Economic Development, 5(1), pp. 1-13.
99. Morris, T. and Wood, G. (2015) 'The value of secondary data in business and management research', Global Business Review, 14(4), pp. 78–92.
100. Motadata (2025) 'Challenges of Digital Transformation in Banking'. Available at: https://www.motadata.com/blog/challenges-of-digital-transformation-in-banking/ [Accessed: 5 February 2025].
101. Moyo, S. & Chikodzi, D., 2023. The impact of digital transformation on banking sector efficiency in Zimbabwe. African Journal of Finance and Management, 32(1), pp.45-61.
102. Moyo, S. & Chikodzi, D., 2023. The impact of digital transformation on banking sector efficiency in Zimbabwe. African Journal of Finance and Management, 32(1), pp. 45-61.
103. Moyo, T. and Ncube, M. (2019) 'Insider threats: A growing concern for financial institutions', African Journal of Information Systems, 11(1), pp. 23-37.
104. Mpofu, J. and Bello, A. (2021) 'Cybersecurity threats in Zimbabwe's banking sector: An overview', International Journal of Cybersecurity, 4(3), pp. 78-90.
105. Muganyi, P. (2022) 'Cybercrime in Zimbabwe: An analysis of the legal framework', Journal of African Law, 66(1), pp. 34-53.
106. Muganyi, P. (2022) 'Cybercrime in Zimbabwe: An analysis of the legal framework', Journal of African Law, 66(1), pp. 34-53.
107. Muguto, T. and Muzindutsi, P.F., 2017. Digital transformation and customer satisfaction in Zimbabwean banks. International Journal of Business and Management Studies, 9(2), pp.45-58.
108. Muteba, M. (2020) 'Digital transformation in Zimbabwean banks: Challenges and opportunities', Journal of Business and Economic Development, 5(2), pp. 1-13.
109. Muteba, M. (2020) 'Digital transformation in Zimbabwean banks: Challenges and opportunities', Journal of Business and Economic Development, 5(2), pp. 1-13.
110. Muteba, M. (2020) 'Digital transformation in Zimbabwean banks: Challenges and opportunities', Journal of Business and Economic Development, 5(2), pp. 1-13.
111. Myke-Okoi Okpa, M. (2022) 'An Assessment of Cyber Crime in Commercial Banks in Calabar Metropolis', Ibom Journal of Social Issues, 11(4), pp. 20–25. DOI: https://doi.org/10.60787/ijsi.v11i4.44.

112. NewsDay Zimbabwe (2024) 'Zim banks vulnerable to cyber threats: Experts'. Available at: https://www.newsday.co.zw/business/article/200033284/zim-banks-vulnerable-to-cyber-threats-experts (Accessed: 16 January 2025).
113. NIST (2023) 'Framework for Improving Critical Infrastructure Cybersecurity'. Available at: https://www.nist.gov/cyberframework (Accessed: 29 January 2025).
114. NIST (2023) 'Framework for Improving Critical Infrastructure Cybersecurity'. Available at: https://www.nist.gov/cyberframework (Accessed: 29 January 2025).
115. Ojo, A.O., et al. (2024) 'Cybercrime in Banking: A Differential Opportunity Perspective', Journal of Financial Crime, 31(1), pp. 45-62.
116. Opdenakker, R. (2006) ‘Advantages and Disadvantages of Four Interview Techniques in Qualitative Research’, Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 7(4). Available at: http://www.qualitative-research.net/index.php/fqs/article/view/175/391 (Accessed: 16 May 2025).
117. Otero, A. R. (2019) 'Digital transformation and cybersecurity: A review of the literature', Journal of Information Systems and Technology Management, 16(1), pp. 1-20. doi: 10.4301/S1807-1775201916010
118. Otero, A.R. (2019) 'Digital transformation and cybersecurity: A review of the literature', Journal of Information Systems and Technology Management, 16(1), pp. 1-20.
119. Publicis Sapient (2023) The Digitalization of Commercial Banking. Available at: https://www.publicissapient.com/content/dam/ps-rebrand/industry/financial-services/2023/GBBS-commercial-banking-report.pdf [Accessed: 5 February 2025].
120. Raimond, P. (2013) Effective research methods: Utilizing secondary data. London: Sage Publications.
121. Reserve Bank of Zimbabwe (2021) Annual report on cybersecurity in the banking sector. Harare: RBZ Publications.
TechZim (2022) ‘Zimbabwean bank hit by ransomware attack’, TechZim, 15 March. Available at: www.techzim.co.zw (Accessed: 20 October 2023).
122. Saunders, M., Lewis, P. and Thornhill, A. (2019) Research Methods for Business Students. 8th edn. Harlow: Pearson Education.
123. Saunders, M., Lewis, P. and Thornhill, A. (2023) Research methods for business students. 9th edn. Harlow: Pearson Education.
124. Scott, W.R. (2021) Organizations: Rational, Natural and Open Systems. 6th edn. Upper Saddle River: Pearson.
125. Sibanda, N., Mutsvangwa, T. & Nyoni, T., 2024. Trends and challenges in the digitalisation of Zimbabwe’s banking sector. International Journal of Banking and Finance, 18(1), pp.88-102.
126. Sibanda, N., Mutsvangwa, T. & Nyoni, T., 2024. Trends and challenges in the digitalisation of Zimbabwe’s banking sector. International Journal of Banking and Finance, 18(1), pp. 88-102.
127. Smith, J., Brown, K., and Taylor, R. (2022) ‘The role of secondary data in understanding digital transformation in banking’, Journal of Financial Technology, 10(1), pp. 45–63.
128. Creswell, J.W. and Creswell, J.D. (2018) Research design: Qualitative, quantitative, and mixed methods approaches. 5th edn. Thousand Oaks: Sage Publications.
129. Gujarati, D.N. (2020) Essentials of econometrics. 6th edn. New York: McGraw-Hill Education. Martin, W.E. (2020) Foundations of sampling and statistical theory. 3rd edn. London: Routledge.
130. Bryman, A. (2016) Social research methods. 5th edn. Oxford: Oxford University Press. Hürlimann, M. (2019) Explanatory research: Methods and applications. Berlin: Springer.
131. Software Mind (2024) 'Leveraging AI for enhanced cybersecurity in banking'. Available at: https://softwaremind.com/blog/leveraging-ai-for-enhanced-cybersecurity-in-banking
132. South African Banking Risk Information Centre (2021) Card Fraud in South Africa. South African Banking Risk Information Centre.
133. Techtarget.com (2024) What is the Electronic Discovery Reference Model (EDRM)? Available at: https://www.techtarget.com/searchcio/definition/EDRM-electronic-discovery-reference-model (Accessed: 3 February 2025).
134. UK Cards Association (2020) Fraud on UK Cards. UK Cards Association.
135. Venkatesh, V. and Bala, H. (2023) 'Technology Acceptance Model 3 and a research agenda on interventions', Decision Sciences, 54(2), pp. 273-315.

136. Venkatesh, V. and Bala, H. (2023) 'Technology Acceptance Model 3 and a research agenda on interventions', Decision Sciences, 54(2), pp. 273-315.
137. VisualSP (2024) 'Digital Transformation in Banking: A Comprehensive Guide'. Available at: https://www.visualsp.com/blog/digital-transformation-in-banking/ (Accessed: 25 January 2025).
138. Wang, Y.S. (2023) 'The impact of perceived risk on users' acceptance of mobile banking', International Journal of Information Management, 38(1), pp. 78-87.
139. Wang, Y.S. (2023) 'The impact of perceived risk on users' acceptance of mobile banking', International Journal of Information Management, 38(1), pp. 78-87.
140. Wolfe, D.T. and Hermanson, D.R. (2023) 'The Fraud Diamond: A New Perspective on Fraud Prevention', Journal of Forensic Accounting Research, 8(1), pp. 45-60.
141. Zawadzki, P., et al. (2022) 'Regulatory compliance and its impact on technology adoption in banking', Journal of Banking Regulation,23(1),pp.56-72.
142. ZICT (2020) Cybercrime in Zimbabwe: A Growing Concern.ZICT (2020) Cybercrime in Zimbabwe: A Growing Concern. Zimbabwe Information and Communication Technologies