Cybersecurity Risks and Mobile Banking Usage in Tanzania

By

Emmanuel Lameck Mkilia

PhD, Moshi Co-operative University

[2024]

Extended Abstract

Technological advancements have transformed how financial institutions manage services and engage with clients. Commercial bank customers can use ICT systems and devices to conduct transactions like balance inquiries, bill payments, and fund transfers electronically. However, integrating ICT into their operations can make banks' and customers' information accessible to third parties, exposing them to cybersecurity risks. The harmful consequences of cybercrime in banking include credit card fraud, spamming, e-money laundering, fraud, phishing, identity theft, and denial of service attacks. This study analysed how cybersecurity systems in various aspects are associated with mobile banking usage among commercial bank customers in Tanzania. Specifically, the study first analysed drivers associated with cybercrime incidences and the usage of mobile banking services. Secondly, the study examined cybersecurity dynamics affecting commercial bank customers' decisions to use mobile banking services. Thirdly, the study determined the association between customers' perceptions of banks' cybersecurity systems and usage of mobile banking services. Lastly, the study evaluated the effect of customers' cybersecurity risk-protective behaviour on the usage of mobile banking services. In attaining these objectives, the study adopted six theories to explain variations in mobile banking usage among customers based on the prevailing status of cybersecurity risks associated with mobile banking in banks. The adopted theories were The Fraud Triangle Theory, Routine Activity Theory, Trust Theory, Extended Parallel Process Model, Unified Theory of Acceptance and Use of Technology and Protection Motivation Theory. By adopting the survey method, a sample of 478 bank customers was collected using a self-administered structured questionnaire. PLS-SEM was used to analyse the link of constructs regarding cyber security risks and usage of mobile banking in Tanzania. This study was to test the predictive relations and clarify the changes in the dependent variables as justified by independent variables; PLS-SEM was regarded as suitable for data analysis. In analysing the influence of cybersecurity risks on the usage of mobile banking services, findings on trends and the

magnitude of cybercrime incidences in Tanzania from 2016 to 2020 indicate that the maximum number of financial cybercrimes occurred in the last quarter of 2016. The increase in cybercrime incidences was associated with the introduction of mobile banking applications and the integration of mobile banking with third-party mobile money agents and applications such as M-Pesa, Airtel Money, Tigo Pesa, Z-Pesa, and T-Pesa. Further, the emergency of agency banking and the launch of a government payment gateway increase the use of mobile services, providing new opportunities and vulnerabilities of mobile devices for cybercriminals to carry out their activities. Further, the findings reveal that customers' self-assessment, customers' decision to take risks, and customers' confidence and trust in mobile phone applications positively affect mobile banking services usage, while access to passwords negatively and significantly affect mobile banking services usage among customers. The study also analysed the influence of banks' cybersecurity systems on mobile banking usage. The analysis was performed to assess how the four dimensions of the UTAUT, that is, performance expectancy, effort expectancy, social influence, and facilitating conditions, influence mobile banking usage. Findings show that all four dimensions of the UTAUT influence mobile banking usage among commercial bank customers. Lastly, the study analysed the commercial banks' customers' cybersecurity protective behaviour when using mobile banking services. The findings indicate that customers' protective behaviour in such aspects as perceived threat, perceived confidentiality, security awareness and perceived self-efficacy positively affect mobile banking services' usage. However, one aspect, perceived severity, significantly negatively affect mobile banking usage. The study recommends that extensive use of mobile banking services and the increasing reliance on technology for financial transactions must coexist with strategies, policies, and readiness to reduce instances of cybercrime. Furthermore, banks should raise security awareness among bank customers by educating them about safe online practices like password management, using trusted networks, and avoiding questionable links. Lastly, there should be collaboration among financial institutions, government organisations, law enforcement, and mobile banking service providers to develop a comprehensive strategy for addressing cybercrime incidents relating to mobile banking usage. This may call for sharing threat and vulnerability data and creating cyber security best practices.

Keywords: Cybercrime, financial institutions, government, organisations, mobile banking usage, cybersecurity