African Journal of Business & Development studies Volume 2 Issue 1 2025
ISSN: 3079-6903
DOI: https://doi.org/10.70641/ajbds.v2i1.155

AFRICAN JOURNAL
OF BUSINESS AND DEVELOPMENT STUDIES

AJBDSresearchjournal@usiu.ac.ke
journals.usiu.ac.ke

Influence of Cybersecurity Risk on Financial Stability of Deposit Taking SACCOs in Kenya

[1*] *Edah Kavwanyiri,* [2]*Elizabeth Kalunda &* [3]*Timothy C. Okech*
[1,2,3] *United States International University –Africa, Nairobi, Kenya*
[1]edah.ke@gmail.com [2]ekalunda@usiu.ac.ke [3]tcokech@usiu.ac.ke

Correspondence Email: edah.ke@gmail.com

Cite: Kavwanyiri E., Kalunda E., & Okech T.C. (2025). Influence of Cybersecurity Risk on Financial Stability of Deposit Taking SACCOs in Kenya. *African Journal of Business & Development Studies*,2*(1),*428-440. https://doi.org/10.70641/ajbds.v2i1.155

Abstract

This study examines the influence of cybersecurity risk on financial stability of Deposit Taking Savings and Credit Co-Operative Society in Kenya. Using explanatory research design, data was obtained from 217 respondents comprising head of risk, head of ICT and business innovations, finance manager and executive- SACCO board member. The study explored how management capability indicator was influenced by ransomware, phishing and distributed denial of service. The gathered quantitative data was analyzed by use of descriptive and inferential statistics. Regression analysis revealed that cybersecurity risk had a moderate negative statistically significant influence on financial stability of DT-SACCOs in Kenya (β = -0.280, R = - 0.268, t = -4.077, p= 0 .000, < 0.05). The implication of the findings is that, as cybersecurity risk decreases, there would be an increase in financial stability. The study therefore recommends management of DT-SACCOs to greatly invest in cybersecurity infrastructure and align clear policies and procedures to curb attacks.

Key Words: Financial Stability, DT-SACCOs, Kenya, Cybersecurity Risk.

Introduction

Recent advances in innovative technology have led to the rapid development and expansion of new financial service (Palmié et al., 2020). Researchers and practitioners consider that innovativeness can reshape the future of Deposit- Taking Savings and Credit Cooperative Society (DT-SACCOs) also known as Credit Unions, though, this is still in doubt because it entails cybersecurity risk posing financial stability threats (Ryu, 2018). Cybersecurity risk refers to the financial loss, disruption or reputational damage to a firm resulting from the failure of its Information technology systems (Stanikzai & Shah, 2021).

According to Farber et al. (2019) managing financial stability of financial institution involves development, use of techniques and systems for rational strategic planning. However, over the past years, DT-SACCOs are experiencing financial instability due to increased cybersecurity risk, and may be more vulnerable than larger institutions due to costly preventive measures (Adeyoju, 2021). In United States and United Kingdom, Trend Micro report showed that Savings and Credit Co-operative Societies (SACCOs) have seen a more than 1,300 increase in ransomware attacks alone in the first half of 2021, compared with the first six months of 2020 (Beaman et al., 2021). Furthermore, cybersecurity programs represented 7.9% of credit union operating budgets in 2021. That figure is a record-high level and a sharp increase from just four years prior, when the average respondent devoted 5.6 percent of the operating budget toward cybersecurity. According to Dunne and Kasekende. (2018) if proper attention is not paid to cybersecurity risk in Africa, future monetary policy initiatives and direction may be negatively impaired.

Kenya is among the most advanced markets in the world in terms of financial technology thanks to the dominance of mobile money (Wachira & Njuguna, 2023). However, most regulations governing the SACCOs were designed with traditional, brick and mortar financial institutions in mind, so they can be burdensome for digital adoption (Musamali et al., 2023) and (Hakizimana et al., 2023). In Kenya, SACCOs are registered under the SACCO Societies Act 2008 (Victor Omollo, 2016). They are licensed, regulated and promoted by the SACCO Societies Regulatory Authority (SASRA) Cap 490. The Act provides minimum requirements for operation and prudent standards necessary for SACCOs that take deposits to minimize risk and ensure stability in funds of the SACCOs.

Kenya's SACCO industry is among the biggest in Africa with 5.7 percent of total assets to GDP ratio, followed by Rwanda and Ethiopia, with 3.0 percent and 0.7 percent, respectively (*SASRA, 2023*)The SACCO industry in Kenya has been faced with back-and-forth cybersecurity risks affecting their financial stability. In 2021, cyber criminals hacked the databases of 3 SACCOs leading to loss of millions of shillings (*CBK, 2023*). Hence, SACCOs are being challenged to review their information technology systems and take insurance covers on the back of cyber-attacks that have in the recent spate of attacks cost them Sh106 million (*SASRA, 2022*). According to the Central Bank of Kenya (*CBK, 2023*), DT- SACCOs lack the necessary financial capacity to acquire appropriate core banking software, inadequate liquidity reserves to facilitate inter-lending among others. This study therefore, focused on the influence of cybersecurity risk on financial stability of DT- SACCOS in Kenya as this significant concept has been deserted by various studies such as Ibrahim, (2018) who focused on financial performance.

Statement of the Problem

Financial stability plays a significant role in economic development and leads to sustained growth fostering to its gradual emergence as a distinct policy function (Muriungi & Waithaka, 2017). Despite the fact that DT-SACCOs are striving to enhance financial stability, they have been stunned due to slow growth to curb cybersecurity risks (Anand et al., 2022). In April 2020, the Financial Stability Board cautioned that cybersecurity occurrence, if not suitably shielded, could extremely interrupt financial structure leading to extensive financial stability implications. Moreover, a study conducted by Tariq, (2018) recognized the significant rapid growth of cybersecurity risk on financial firms which requires financial institutions to heighten cybersecurity audit on an ongoing basis and stiffen security countermeasures to enrich financial stability. According to Shehab et al. (2024) the most common identified cybersecurity risk in credit union sector are worms, ransomware, phishing and distributed denial of service (DDoS) attacks.

In the same way, Wang et al. (2020) established that cybersecurity risk has become a key problem for Nigeria's financial sector with the biggest incidences' being phishing and D-Dos attacks. In the year 2023, National Credit Union Administration reported that credit unions incurred significant number of cybersecurity attacks, with approximately reported incidents of 892 between year 2023 September and May 2024. However, despite SASRA partnering with other relevant government agencies such as the Financial Reporting Centre (FRC), the Office of Data Protection Commissioner (ODPC), the Ethics & Anti-Corruption Commission (EACC) and the Communications Authority of Kenya (CA) in year 2023 to deliver tailor made capacity building and sensitization programs on such emergent cybersecurity framework, the sector has not enhanced its financial stability. Based on the literature, DT-SACCOs are exposed to high threats cybersecurity risk and attacks as they encompass highly profound and intimate member data, this research therefore sought to fill the gap and examined the influence of cybersecurity risk on financial stability of Deposit Taking- SACCOs in Kenya.

The study is hypothesized as follows:

H_0: Cybersecurity risk has no statistically significant influence on financial stability of Deposit Taking SACCOs in Kenya.

Literature Review

This section provides the theoretical, empirical, and conceptual framework that guided the study.

Theoretical Review

This study adopted Theory of Financial Intermediation and Risk Management Theory. Developed by Marty (1961) , the theory of Financial Intermediation is based on informational asymmetry theory and the agency theory information. The theory draws relevance from the concept of resource allocation. It further proposes that there exist instabilities such as information asymmetry and transaction costs that are crucial in articulating and upholding financial stability (Merton, 1995). The Agency relationship explains how returns can enhance financial stability. Evolving through contributions from various thinkers and institutions, risk management theory is used by firms to identify, monitor, assess, and manage risk (Pyle ,1997). Therefore, the relationship between these theories and cybersecurity risk is that threats and vulnerabilities regarding information security could be estimated and assessed in firms to strengthen financial stability.

Empirical Review

The identification of cybersecurity risk is vital to financial institution stability. According to Andia (2024) management should always develop a model encompassing corporate governance, Information system controls, human resource management, strategic planning and audit programs to measure financial stability. DT-SACCOs are exposed to high threats of cybersecurity risk and attacks as they encompass highly profound and intimate member data hence the essence of robust cybersecurity review. In this perspective, Uddin et al. (2020) claim that unauthorized access and disclosures, misuse of data or information and organized attacks in form of introduction of malware and similar extraneous viruses lead to

cybersecurity threats impeding financial system stability. Similar concern has also been expressed by (Anand et al., 2022) who stated that a successful invasion and deployment of ransomware may interrupt operations for all banking sector. Also, Bhavsar et al. (2018) determined that ransomware, phishing and D-DOS attacks can result in significant disruptions to business operations and substantial financial losses. It is therefore very important that organizations pay attention to end-user awareness to prevent cybersecurity threat due to the growth of internet technology which causes security threats to systems and networks (Gupta et al., 2017) .

With this in view, Jameaba (2022) analyzed how cybersecurity influenced financial stability of Indonesian banking industry for the period 2014 to 2021 through a Laku Pandal, that is, a branchless Program assessing 13 national banks. The researcher adopted qualitative research design implemented using documented analysis by assessing or eliciting available data. Documents analysed included magazines, journals articles, regulations, relevant book chapters, circulars, reports, chronicles, webinars, podcasts and relevant document source application. The researcher found that cybersecurity aggregated platforms that standardize and automate financial data leading to resilience in the event of financial stress. The study recommended that adequate regulatory frameworks need to be underlined.

While Aldasoro et al. (2020) investigated the influence of cybersecurity risk as one of the operational risk on financial stability within large, medium and small banks in United States, Canada, Southern Europe, Northern Europe, United Kingdom and Western Europe from 2002: Q1 to 2018: Q3. The full sample comprised over 700,000 observations of operational loss events, however, the study worked mainly with a sample of 521,082 incidents which was obtained after combining individual loss data with region and bank size data and truncating data at 2016: Q4. Data collected was owned, managed by ORX and anonymized. Despite finding that cybersecurity risks affect major payments system, or corrupts the data of a major financial institution or data provider, the anonymization of data causes inaccuracy and implementation complexity. This study therefore seeks to fill this gap by using regression analysis as opposed to being managed by ORX.

The concept of ransomware has greatly been linked to financial stability. According to Krivokapić et al. (2023) who determined how financial stability in Republic of Serbia from 2019 to 2022 is impacted by ransomware threats. Findings stipulated that, ransomware lead to various losses, that is, Loss of customers, investigation costs, verification costs to check systems, restoration costs to put systems back online and Loss of reputation. The mix formal dogmatic methodological approach used by the study seeks to be filled as a gap by this study through adopting explanatory research design which concentrate on facts (Legowo et al., 2020). Despite the fact that the study of Shehab et al. (2024) conducted from year 2008 to 2022 to investigate how malware attacks affects financial institutions stability it only used qualitative data which was analysed using content analysis. Therefore, this study has a broader perspective in terms of conceptual and contextual framework by examining the influence of cybersecurity risk on financial stability of DT-SACCOs in Kenya.

Conceptual Framework

This study is underpinned by a conceptual framework, shown in Figure 1, which illustrates how cybersecurity risk influence financial stability. In this context, cybersecurity risk refers to a series of hazards posed on practices and activities fashioned out with a view to ensuring the protection of members' data, information and networks from all possible threats whether internally or externally induced to achieve financial stability through implementing rational strategic planning of financial solution.

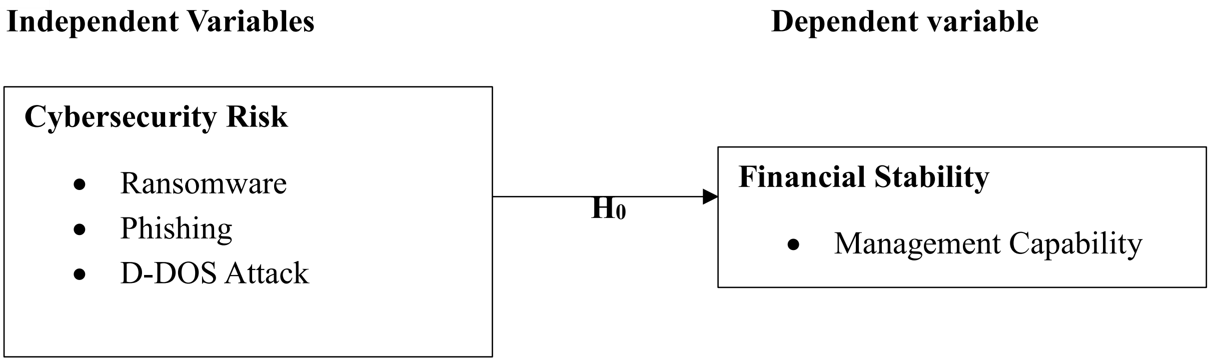

Figure 1: Conceptual Framework

Ransomware, phishing and D-DOS attacks were used to measure cybersecurity of DT-SACCOs in Kenya. This is in accordance of a principal-agent model adopted by Ahnert et al. (2022) in Canada where fee-paying clients who delegate security decisions to financial platforms face cybersecurity risk. To achieve financial stability, it is essential to determine the critical mechanisms influencing them (Bashir, 2021). Farber et al., (2019) states that to manage financial stability of financial institutions, the development and use of systems and techniques for rational strategic planning of financial solutions need to be implemented. Management capability was used to measure the financial stability assessed through the management practices which include corporate governance, information system controls, HRM, strategic planning and audit programs.

Research Methodology

This study was anchored on research philosophy pursued by positivism and employed explanatory research design. With a sample size of 256 respondents, this study used cross sectional survey to collect primary data using a standard questionnaire from four respondents encompassing head of risk, head of ICT and business innovations, finance manager and executive- SACCO board member in selected DT-SACCOs in Kenya. To help ensure a more representative sample, purposive sampling was further adopted in selecting study participants who were considered to be knowledgeable of the variables under study from year 2018 to 2023. This study adopted SPSS Version. 26 to generate inferential and descriptive statistics which were presented in forms of table formats and graphs. Pilot study was conducted by submitting research questionnaire. The study was reliable since all the variables attained reliability threshold with a Cronbach's alpha reliability of greater than 0.5. The measure items met the validity criteria as they all had an Average Variance Extracted of above 0.5. Before conducting the regression analysis, diagnostic tests were conducted to evaluate normality test, linearity test, heteroscedasticity test and collinearity test. The study adopted the ordinary least square regression model for inferential statistics.

Study Results and Discussion

General Information

The study gathered primary data of cybersecurity on financial stability from 256 DT-SACCOs respondents in Kenya for a period of 5 years (2018 – 2023). 217 study participants responded to the questionnaire adequately, giving a response rate of 84.8 percent. The response was considered adequate as it was well over the recommended 60 percent (Saunders et al., 2019). Majority of the study respondents 58.1 percent were male, while 41.9 percent were female. Most of the study respondents 49.8 percent were between the ages of 35 and 44 years, 28.1 percent were between the age 25 to 34 years, 16.1 percent were between 45 to 54 years, 3.7 percent were below 25 years while 2.3 percent were above 55 years of age.

Findings indicated that majority of the respondents 27.6% were head of risk, followed by 26.7 who were finance managers, 24.9% were head of ICT and business innovations and 20.7% were executive- SACCO board members.

These findings indicate that the information provided by the respondents can be highly reliable to the study. The findings also showed respondents that participated in the study had attained high education levels and thus were in a good position to engage and provide the required information. Further, 44.7 percent of the study participants had been working in the DT-SACCO for a period of 5 to 10years and 44.2 percent have worked for more than 10 years. These findings imply that the study respondents had relatively good work experience that would enable them to respond effectively.

Descriptive Analysis of Variable Measure

Data was collected using a 5-point Likert scale where respondents were required to rate their level of agreement with statements on a scale of 5, with one indicating strong disagree and five indicating strong agree. Management capability was used to measure financial stability. Descriptive statistics of the means (M) and standard deviations (SD) were used to analyze the responses, with mean values of 1.0-1.80 representing strongly disagree; 1.81-2.60 representing disagree; 2.61-3.40 representing neither agree nor disagree; 3.41-4.20 representing agree, and 4.21-5.0 representing strongly agree. The results of the SD that is less than 1 is interpreted as being closely dispersed around the mean, whereas the SD greater that 1 is interpreted as responses being high dispersed away from the mean. Table 1 shows the mean and standard deviation of management capability measures for financial stability.

Table 1. Adoption of Financial Stability

Management Capability	Mean	Std. Deviation
Management of my DT- SACCO maintain high standards of professionalism by ensuring performance standards are in place to enhance a positive significant financial stability.	3.00	0.481
To prioritize a stable financial system, management of my DT-SACCO ensure effective security information controls are in place to safeguard members' investments and data.	3.00	0.544
My DT-SACCO employees are thoroughly trained on specific daily operations to meet the needs of the firm so as to improve financial stability.	4.12	0.460
I can tell that robust strategic plan developed by management can provide resilience to financial system hence strengthening financial stability.	3.00	0.529
To ensure financial stability, my DT-SACCO audit programs independently, report to the supervisory committee without interference from management.	3.02	0.504

Cybersecurity Risk and Financial Stability

This section covers the descriptive analysis of the primary data gathered in the study on the influence of cybersecurity risk on financial stability of DT-SACCOs in Kenya. The measurements under cybersecurity risk variable were Ransomware, Phishing and D-DoS Attack.

Table 2. Cybersecurity Risk and Financial Stability

Questionnaire Items on Cybersecurity Risk	Mean	Std. Deviation
Ransomware		
My DT-SACCO is highly exposed to malicious software hence deny users access to information systems.	2.98	1.425
Although ransomware have not been systemic, severe incidents at my DT-SACCO cause loss of confidence to clients.	2.97	1.445
My DT-SACCO financial stability weakens due to high cost caused by ransomware because the hackers use technologies that provide them with the ability to hijack database information.	3.07	1.409
A ransomware attack at my DT-SACCO can threaten financial stability through lack of substitutes for the services rendered.	2.99	1.419
Ransomware are a key operational risk that threaten my DT-SACCO operational resilience, affecting overall financial stability.	2.94	1.452
Phishing		
Phishing leads to monetary losses at my DT-SACCO as the fraudsters take the money.	3.22	1.409
Growth of Internet technology has resulted to increased phishing threats to systems in my DT-SACCO.	3.01	1.424
My DT-SACCO can increase its ability to absorb shocks if efficiency of spam filters is improved.	3.01	1.416
My DT-SACCO develop context-based education for employees to decrease phishing exposure thereby stabilizing financial system.	3.01	1.414
D-DoS Attack		
The ability of attackers to disable information technology systems used by my DT- SACCO is a threat to financial stability.	3.09	1.440
My DT-SACCO is equipped with sufficient resources and backups so that services may still be available for users in case of an attack to portray a positive financial stability.	2.98	1.421

My DT-SACCO has a well-defined incident response plan in place to quickly mitigate the impact of a DDoS attack, reducing financial system vulnerability.	3.02	1.427
Periodic security audits help my DT-SACCO to identify weak points in defence systems and take corrective action before an attack occurs.	3.01	1.473

The Pearson correlation analysis was used to understand the strength and direction between cybersecurity risk and financial stability as shown in Table 3. The results indicate a moderate negative correlation between cybersecurity risk and financial stability. The correlation coefficient is -0.268 and the p-value is less than 0.05, suggesting that this negative relationship is statistically significant (r = - 0.268, p = 0.000). These findings imply that as cybersecurity risk decreases, there would be an increase in financial stability and vice versa.

Table 3: Correlation Between Cybersecurity Risk and Financial Stability

		Cybersecurity Risk
Financial Stability	Pearson Correlation	-0.268**
	Sig. (2-tailed)	0.000
	N	217

**. Correlation is significant at the 0.01 level (2-tailed).

Diagnostic Tests for OLS Regression

This research used regression analysis to test hypothesis of the relationship between cybersecurity risk and financial stability of Deposit Taking SACCOs in Kenya. Prior to fitting the model, diagnostic tests were conducted to confirm the suitability of the data for modelling. Findings indicated that the items used to measure the variable of cybersecurity risk did not exhibit any substantial deviation from a normal distribution. None of the relationship tests had a VIF above 5, they ranged between 1.028 and 1.099 indicating that no multicollinearity.

Regression analysis Model Coefficient of Cybersecurity Risk on Financial Stability

Regression analysis model accurately represented and fitted the data as shown by the p statistic (p < 0.05). Hence cybersecurity risk adds a substantial contribution to explaining financial stability of DT-SACCOs in Kenya. The findings revealed a negative statistically significant influence of cybersecurity risk toward financial stability at a 5 percent significance level (t = -4.077, p < 0.05).

The general form of the equation to predict financial stability from cybersecurity risk was;

husband's years of education, is

$$\textit{Financial Stability} = 2.655 - 0.280\ (\textit{Cybersecurity Risk}) + E$$

The constant term 2.655, is the predicted value for the dependent variable (in this model) financial stability if independent variable, cybersecurity risk = 0. That is, we would expect financial stability of 2.655 when predictor variable, cybersecurity risk takes the value 0. For this reason, this is only a meaningful interpretation if it is reasonable that the predictor can take the value 0 in practice. Unstandardized coefficients indicate how much the dependent variable varies with an independent variable when all other independent variables are held constant.

The regression coefficient provides the expected change in the dependent variable, financial stability, for a one-unit increase in the independent variable, cybersecurity risk. Referring to the coefficient in Table 4, the unstandardized coefficient for cybersecurity risk is – 0.280. This means for every unit increase in cybersecurity risk, there is 0.280 decrease in financial stability.

Table 4. Regression analysis Model Coefficient of Cybersecurity Risk on Financial Stability

Model	Unstandardized B	Std. Error	Standardized Beta	t	Sig.
Constant	2.655	0.090		29.552	0.000
Cybersecurity Risk	-0.280	0.069	-0.268	-4.077	0.000

Regression Model Summary of Cybersecurity Risk on Financial Stability

Findings shows that the coefficient of determination is 0. 072. This means that the effect of the predictor/independent variable; Cybersecurity risk explains approximately 7.2% of the variations in Financial Stability of DT-SACCOs in Kenya. Therefore, from the analysis, Cybersecurity risk has a moderate negative correlation against Financial Stability and the Durbin Watson value of 1.822 indicated there was no autocorrelation since the value was between 1 and 3.

Table 5. Regression Model Summary of Cybersecurity Risk on Financial Stability

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.268[a]	0.072	0.067	0.40417

ANOVA for Cybersecurity Risk

The F-ratio in the ANOVA tests whether the regression model is a good fit for the data. The findings showed that the independent variable, cybersecurity risk statistically significantly predicted the dependent variable, F (1, 215) = 16.625, p (.000) < .05. Therefore, the regression model is a good fit of the data and that cybersecurity risk is significant in determining financial stability of DT-SACCOs in Kenya. As a result, the null hypothesis,

H_0: Cybersecurity risk has no statistically significant influence on Financial Stability of Deposit Taking SACCOs in Kenya, was rejected and the alternative hypothesis was supported.

Table 6. ANOVA of Cybersecurity Risk on Financial Stability

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	2.716	1	2.716	16.625	0.000^b
Residual	35.121	215	0.163		
Total	37.837	216			

Discussion of Results

The findings indicated that cybersecurity risk had a negative statistically significant influence on financial stability of DT-SACCOs in Kenya. Equating these results with preceding research discloses fascinating outlines on the relationship between cybersecurity risk and financial stability. Shehab et al. (2024) examined how cybersecurity risks and threat affect financial stability the banking sector. The study stated most common types of attacks used to breach protected financial data are "malware attacks (ransomware, phishing attempts, viruses, and worms), distributed denial of service (DDoS), conveyed denial of service (CDoS), money theft, identity theft, money laundering, data leakage, social engineering attacks, hacking/IT incidents, unauthorized access, data loss or theft, impersonating, and SMS spoofing". Despite theoretical and methodological deviation, as the study adopted routine activity theory and questionnaires were used for data collection; quantitative data was analysed using SPSS and information was obtained from key informants, the findings of Shehab et al. (2024) aligned with this study as cybersecurity threat also had a negative influence on financial stability. However, this study finding partially contradicts the findings of Aldasoro et al. (2020) who indicated that cybersecurity risk had a positive statistically significant influence on financial stability within large, medium and small banks in Europe from 2002 to 2018. The study also raised some questions on methodological deviation, whereas it focused exclusively on the Bayesian methodology with a sample size of 521,082 respondents. This study used a sample size of 256 respondents calculated using the Yamane formula. This therefore suggests that the impact of cybersecurity risk may vary across different financial contexts while maintaining either positive or negative significant influence.

Conclusion

This research has demonstrated a composite relationship between cybersecurity risk and financial stability of DT-SACCOs in Kenya. Findings suggest that the effects of ransomware, combined with phishing and D-Dos Attack if not well managed can cause a threat to a DT-SACCO. The study revealed that cybersecurity risk had a negative significant part in influencing financial stability of DT-SACCOs in Kenya. Besides, the research showed a moderate negative significant correlation between cybersecurity risk and financial stability. The study, therefore, rejected the null hypothesis and concluded that cybersecurity risk has significant influence on Financial Stability of Deposit Taking SACCOs in Kenya.

Limitations of the study

This study has limitations that could be addressed in future research. The adoption of questionnaire is subject to limited depth due to closed-end questions and the general incapability to shed light on ambiguous responses. The cross-sectional design also has a higher risk and prevents causal inference between exposure and outcome. By addressing these limitations, future researchers may provide more methodological insight.

Recommendation

This research highlights the need for exploration into the various ways in which cybersecurity risk influence financial stability of deposit taking SACCOs in Kenya. In light of the research findings, it is recommended that management of DT-SACCOs should greatly invest in cybersecurity, adequate information technology infrastructure should be put in place, clear cybersecurity policies and procedures should be aligned to regulate access to personal data by only authorized persons. Management should also develop context based education to employees in regard to cybersecurity to curb attacks. Further, management can procure cybersecurity insurance to cover liability resulting from an attack more so if they are dealing with sensitive data. Future studies should also explore the use of other primary data collection methods, for example case studies, interviews and focus group discussions, to get more discernments.

References

Adeyoju, A. (2021). Cybercrime and Cybersecurity: FinTech’s Greatest Challenges. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3486277

Ahnert, T., Brolley, M., Cimon, D., & Riordan, R. (2022). *Cyber Risk and Security Investment*. https://doi.org/10.34989/SWP-2022-32

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). *Operational and cyber risks in the financial sector*.

Anand, K., Duley, C., & Gai, P. (2022). Cybersecurity and Financial Stability. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4073158

Andia, S. (2024). Fraud Prevention Strategies and Financial Stability of Insurance Companies in Kenya. *African Journal of Commercial Studies*, *5*(1), 42–50. https://doi.org/10.59413/ajocs/v5.i1.6

Bashir, Z. (2021). An Empirical Analysis of Working Capital Management Attributes and Firm’s Profitability Evidence from the Textile Sector of Pakistan. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3936363

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, *111*, 102490. https://doi.org/10.1016/j.cose.2021.102490

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on Phishing Attacks. *International Journal of Computer Applications*, *182*(33), 27–29. https://doi.org/10.5120/ijca2018918286

CBK (2023). *Banking Sector Innovation Survey*. https://www.centralbank.go.ke/2023/06/30

Dunne, J. P., & Kasekende, E. (2018). Financial Innovation and Money Demand: Evidence from Sub-Saharan Africa. *South African Journal of Economics*, *86*(4), 428–448. https://doi.org/10.1111/saje.12205

Farber, H. S., Herbst, C. M., Silverman, D., & Von Wachter, T. (2019). Whom Do Employers Want? The Role of Recent Employment and Unemployment Status and Age. *Journal of Labor Economics*, *37*(2), 323–349. https://doi.org/10.1086/700184

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2017). *Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.1705.09819

Hakizimana, S., Makau Charity Wairimu, M.-, & Stephen, M. (2023). Digital Banking Transformation and Performance-Where Do We Stand? *International Journal of Management Research and Emerging Sciences*, *13*(1). https://doi.org/10.56536/ijmres.v13i1.404

Ibrahim, A. M. (2018). *The effect of financial technology on the financial performance of commercial banks in Kenya [Master's thesis, Department of Finance and Accounting University of Nairobi]*.

Jameaba, M.-S. (2022). *Digitalization, Emerging Technologies, and Financial Stability: Challenges and Opportunities for the Indonesian Banking Industry and Beyond*. https://doi.org/10.32388/CSTTYQ.2

Krivokapić, Đ., Nikolić, A., Stefanović, A., & Milosavljević, M. (2023). Financial, Accounting and Tax Implications of Ransomware Attack. *Studia Iuridica Lublinensia*, *32*(1), 191–211. https://doi.org/10.17951/sil.2023.32.1.191-211

Legowo, M. B., Subanidja, S., & Sorongan, F. A. (2020). Model of Sustainable Development Based on FinTech in Financial and Banking Industry: A Mixed-Method Research. *2020 3rd International Conference on Computer and Informatics Engineering (IC2IE)*, 194–199. https://doi.org/10.1109/IC2IE50715.2020.9274605

Li, C., Li, Y., Xu, Y., & Sun, G. (2025). Research on the impact of financial technology on risk-taking of commercial banks. *Research in International Business and Finance*, *76*, 102804. https://doi.org/10.1016/j.ribaf.2025.102804

Marty, A. L. (1961). Gurley and Shaw on Money in a Theory of Finance. *Journal of Political Economy*, *69*(1), 56–62. https://doi.org/10.1086/258414

Merton, R. C. (1995). Financial innovation and the management and regulation of financial institutions. *Journal of Banking & Finance*, *19*(3–4), 461–481. https://doi.org/10.1016/0378-4266(94)00133-N

Muriungi, C. N., & Waithaka, M. (2017). *EFFECTS OF RISK MANAGEMENT ON FINANCIAL STABILITY OF STATE CORPORATIONS IN KENYA: A SURVEY OF TOURISM FUND (TF) AND KENYATTA INTERNATIONAL CONVENTION CENTRE (KICC)*. *2*(3).

Musamali, R., Jugurnath, B., & Maalu, J. (2023). *FINTECH IN KENYA: A POLICY AND REGULATORY PERSPECTIVE*. *8*(1).

Palmié, M., Wincent, J., Parida, V., & Caglar, U. (2020). The evolution of the financial technology ecosystem: An introduction and agenda for future research on disruptive innovations in ecosystems. *Technological Forecasting and Social Change*, *151*, 119779. https://doi.org/10.1016/j.techfore.2019.119779

Pyle, D. H. (1997). *Bank Risk Management: Theory*. Institute of Business and Economic Research, University of California, Berkeley. https://books.google.co.ke/books?id=pNKbHAAACAAJ

Ryu, H.-S. (2018). *Understanding Benefit and Risk Framework of Fintech Adoption: Comparison of Early Adopters and Late Adopters*. Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2018.486

SASRA. (2022). The SACCO supervision annual report, 2022. *The Annual Statutory Report on the operations and performance of SACCO. https://www.sasra.go.ke/30/06/2022.*

SASRA 2023. The SACCO supervision Annual report 2023. *https://www.sasra.go.ke/2023/08/28.*

Shehab, R., S.Alismail, A., Amin Almaiah, Dr. M., Alkhdour, Dr. T., AlWadi, Dr. B. M., & Alrawad, Dr. M. (2024). Assessment of Cybersecurity Risks and threats on Banking and Financial Services. *Journal of Internet Services and Information Security*, *14*(3), 167–190. https://doi.org/10.58346/JISIS.2024.I3.010

Stanikzai, A. Q., & Shah, M. A. (2021). Evaluation of Cyber Security Threats in Banking Systems. *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*, 1–4. https://doi.org/10.1109/SSCI50451.2021.9659862

Tariq, N. (2018). *IMPACT OF CYBERATTACKS ON FINANCIAL INSTITUTIONS*.

Uddin, Md. H., Ali, Md. 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

Victor Omollo, O. (2016). Strategic Factors Affecting Compliance with the Sacco Act of 2008 by Financial Co-operatives in Kenya: A Case of Nairobi County Sacco. *Science Journal of Business and Management*, *4*(3), 90. https://doi.org/10.11648/j.sjbm.20160403.15

Wachira, G., & Njuguna, A. (2023). Enhancing Growth and Productivity Through Mobile Money Financial Technology Services: The Case of M-Pesa in Kenya. *International Journal of Economics and Finance*, *15*(12), 91. https://doi.org/10.5539/ijef.v15n12p91

Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, *62*, 100415. https://doi.org/10.1016/j.ijlcj.2020.100415