The University Journal: A Doctoral Association of Eastern Africa (DAEA) Publication
Vol 7(2)

ISSN: 2519-0997 (Print)

Influence of Data Breach Risk on Financial Stability of Deposit Taking SACCOs in Kenya

Edah Kavwanyiri[1], Elizabeth Kalunda[2] and Timothy. C. Okech[3]
[1,2,3] United States International University- Africa
Email: edah.ke@gmail.com;* ekalunda@usiu.ac.ke; tcokech@usiu.ac.ke

***Corresponding author**

Cite: Kavwanyiri, E., Kalunda, E., & Okech, T.C. (2025). Influence of Data Breach Risk on Financial Stability of Deposit Taking SACCOS in Kenya. *The University Journal, 7*(2), 79-90.

Abstract

This study examines the influence of data breach risk on financial stability of Deposit Taking SACCOs in Kenya. Driven by positivism philosophy and explanatory research design, data was collected from 256 respondents (84.7% response rate) comprising of head of risk, head of ICT and business innovations, finance manager and executive- SACCO board member. Cross sectional data was used and a questionnaire was administered to gather data. The study investigated how hacking, insider threat and unpatched software influenced management capability indicator. Regression analysis revealed a weak negative relationship between data breach risk and financial stability ($R = -0.113$, $R^2 = 0.013$, $\beta = -0.166$, $p = 0.048$, < 0.05), leading to the rejection of the null hypothesis. These findings imply that as data breach risk increases, there would be a decrease in financial stability. The study recommends tracking vulnerability patches, updating Softwares and ensuring enriched patching backup security by management certify a more stable financial system. These findings contribute valuable insights for SACCOs management and regulatory authority seeking to manage potential threats by promoting resilience towards data breach risk through management capability practices.

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

Introduction

In the current digital world, data has become most essential in Deposit Taking SACCOs (DT-SACCOs) also termed as credit unions. To protect this sensitive information, more innovative ideas are coming into existence in the context of data breach (Manju et al., 2022). However, given its ever increasing implementation, the term data breach is still considered as qualm, insofar as the trend of applying advanced technological solutions to the financial sector is still being developed in new ways, this leads to data breach threats affecting financial stability (Gai et al., 2018). Data breach risk is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner (Nzuva, 2019). Online data and sophisticated hacking tools have spurred a steep increase in data breaches (Hope Credit Union, 2023). In Ireland, Data Protection Commission (DPC) noted that on 30 November 2018, it received a personal data breach notification from Slaney Credit Union. The DPC provided that the personal data breach was related to an unauthorized disclosure of personal data in the form of an unintended publication of member data on the internet where certain board reports relating to membership enquiries stored within the Slaney Credit Union website inadvertently became publicly available through search engine results for a period in 2018. The DPC further highlighted that according to Slaney Credit Union, this incident occurred due to an update to a search engine optimization tool installed on the website that Slaney Credit Union had not anticipated (Data Guidance, 2022).

In USA data breaches is a resurging threat for credit unions which keeps them at risk for identity scams, including financial identity theft commonly a form of ID theft (Roy, 2021). First Financial Credit Union ("FFCU"), based in Albuquerque, New Mexico, filed office ail notice of a data breach on its website. This notice explained that an unauthorized party was able to access certain FFCU files containing sensitive member data. More specifically, the leaked information included members' names, addresses, Social Security numbers, government ID numbers, bank account information and credit card information (Console, 2022).

In Kenya there are 176 DT- SACCOs Societies listed and duly licensed to carry out deposit-taking business as provided in the Act and the said Regulations, 2010 (SASRA Annual Report, 2023). Unfortunately, as authorities update their approaches, SACCOs often serve as test cases and must bear the brunt of delays, learning processes, regulatory overheads, overregulation and indecision (Abby,2021). Despite Kenya passing the Data Protection Act 2019, which requires a financial institution to inform the data subject of whom their personal data may be shared, there are no regulations introduced to promote SACCOs to make customer or product data available to third parties of open banking or credit referencing (Rashed, 2019). The Central Bank of Kenya (CBK) in the 2020 Financial Sector Stability Report stated that SACCO systems have very minimal verification by members which makes them easy targets. Moreover, some SACCOs using systems provided by third-party vendors do not even have clauses in their agreement where lost cash can be refunded (Munuve, 2021). In this treaty of emergent data breach risks arising from increased financial technology by DT- SACCOs to deliver financial services and products. Noting that 99% of data breaches on systems have been occasioned through third-party systems vendors and integrators, SASRA developed and issued a Circular on the Minimum Requirements for Engagement with Third-Party System Integrators and Vendors (Ref. SASRA/GG/1/2023 dated 6th June 2023). However, despite the regulation, DT-SACCOs still incur data breach risk.

Statement of the Problem

The importance of DT- SACCOs within the financial industry has increased in recent years, evolving from manual processing, paper transactions to real time account access (Kembo & Mwakujonga, 2022). Experienced with sophisticated range of data breach risk coupled with escalating advancement in financial technology (NCUA report, 2023) DT-SACCOs need to claim vigilance. However, in order to maintain this broader strategic mandate, DT-SACCOs must consider ways to become more effective and streamlined to enhance financial stability.

In Kenya, DT-SACCOs play a vital role in financial intermediation despite the fact that they attract targets for data breaches due to the sensitive financial data they embrace, they hold 6.3% membership of Kenyans and approximately 60% of Kenyans are highly dependent on the firms (FinAccess, 2022). According to SASRA report (2019), DT-SACCOs incurred capital increment from 14.46 percent in 2018 to 15.53 percent in 2019 which could aid to curb shocks. However, in 2019 they experienced a decline in net income from 15.31 percent in 2018 to 13.97 percent in 2019 evidenced by rising data breaches. The ever-changing financial stability within the sector has led to various discussions and literature, for instance, Lars and Morten (2019) conducted a study on data breach and financial stability of 15 financial firms affected by data breaches in Europe countries, findings indicated that, investors value news of a data breach negatively hence strategic measures need to be aligned. Betz (2016) stated that data breaches in the U.S. is an increasing distress for financial services firms due to the likely influence on customer service, loss of reputation, lawsuits and regulatory drawbacks. Regardless of the implementation of Data Protection Act of 2019 in Kenya which require DT-SACCOs to

mandatory comply with its provisions, they still incur data breach risk. This study therefore focused on filling the literature gap and determined the influence of data breach risk and financial stability of DT- SACCOs in Kenya.

The study is hypothesized as follows:

H_0: There is no statistically significant influence of data breach risk on Financial Stability of deposit taking SACCOs in Kenya.

Theoretical Review

Risk Management Theory

This theory has evolved through contributions from various thinkers and institutions. From among the well-known scientists who have contributed to the science of risk management theory underpinning this study is David (1997), aiming to identify how firms can be able to identify, assess, and manage risk. This theory can thereby benefit businesses by protecting themselves from financial losses (Yu, 2021). The essence of this theory underpins the study because the vulnerabilities that could lead to data breaches or other security incidents can endure risk management procedure.

Theory of financial intermediation

This theory was developed by Gurley and Shaw (1960). In principle, the existence of financial intermediaries is explained by the existence of high cost of transaction, inadequate information in useful time and regulation. Further, this theory is grounded on the concept of informational asymmetry theory and the agency theory information. The theory asserts for the presence of financial intermediaries who leverage on the existence of exaggerated transaction costs, asymmetric information, existence of regulations and magnified monitoring costs in the financial sector to enhance stability.

Empirical Review

Lars and Morten (2019) conducted a study on data breach and financial stability of 15 financial firms affected by data breaches from year 2006 to 2018 in Canada, China, France, United Kingdom, Switzerland, Japan and USA. Using qualitative case study, Privacy Rights Clearinghouse database of publicly disclosed data breaches (Privacy Rights Clearinghouse, 2018) was used to ascertain sampling. For the identified firm, public company statements and news articles relating to the data breach were reviewed, to identify the subsequent details about the breach and the actual date of first disclosure that were given such as the type of data that was lost, cause of breach and size. Multiple variable regression was used to test the statistical significance level. Findings indicated that, investors value news of a data breach negatively, as a statistically significant market value loss is present instantly following the discovery of a data breach. The study concluded that, communicative strategy must be reliable with the strategic measures put in place to limit the effects of the threat, otherwise the response may seem dissembling and discordant with the expressive response from clients. Further, the researchers recommended that future studies should focus on analysing the corporate strategies firms select in the wake of data breaches. Moreover, the study did not take into consideration the effect of regulation hence recommended forthcoming studies to be conducted to firms that are breached while the new regulation is in effect.

Jerotich et al. (2019) examined data breaches and financial stability among SACCOS in Kenya. The study used descriptive research design presented by use of frequency tables among 135 SACCOS registered with SACCO Societies Regulatory Authority (SASRA). The study adopted simple random sampling to select 85 SACCOS. Purposive sampling was further used in selecting 85 information technology personnel participants. To collect both quantitative and qualitative data, the researchers utilized questionnaire as the survey instrument. The study recognized that in all the SACCOS studied, data breach policies are used to sustain stability. However, there are still challenges on how data breaches and incidents can be contained based on the findings and therefore calls for further research in academic research.

Jiaojiao (2022) assessed the effect of data breaches in the financial service industry among top-listed United States financial institutions during a nine years' time frame 2010-2018. From the study, among 58 firms, there were 88 data breaches observations. Data was collected from 3rd party analytical channels, companies' public online reports, databases of the global financial news channels, listed companies' earnings and profit reports, Securities and Exchange Commission (SEC) reports and companies' own announcements. These were analyzed to evaluate data breach losses of firms among the top-listed US financial institutions. The study findings stated that, listed firm value was negatively impacted after data breaches. However, a positive impact can be established if the firm increases data breach measures, enhance corporate governance and employ information technology security control manager.

Cansu et al. (2021) studied financial impact of data breaches on financial firms in United states from the year 2001 to 2018. Data from 192 measures were analyzed by employing Event Study Methodology based on quantitative approach. Data was collected secondarily from technology portals, newspapers, a number of IT security-related blogs magazines, various sources through the search engines Google and Yahoo and the website of a nonprofit organization named Privacy Rights Clearinghouse. Findings indicated that financial firms had a significant negative impact to data breaches. In conclusion, financial firms are getting attacked more than any other sector and therefore preventive measures need to be taken.

Conceptual Framework

This study is underpinned by a conceptual framework, shown in Figure 1, which illustrates how data breach risk influence financial stability.

Independent Variables

Dependent variable

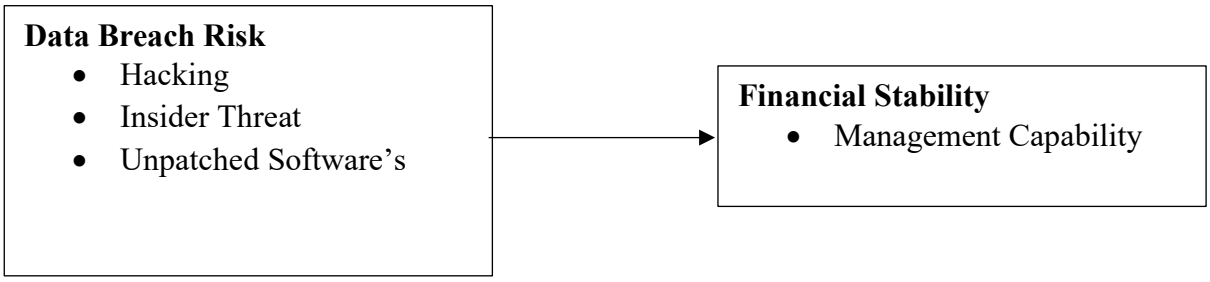

Figure 1: Conceptual Framework

The study measured data breach by analysing hacking, Insider threats and Unpatched software's with financial stability of DT- SACCOs in Kenya. Various researchers have measured financial stability using management capability basing on different models. By exploring existing research findings, we gain valuable insights into how this measure interact and influence financial stability. Penny, Jim and Rebecca (2002) developed a model on how management capability measures financial stability in UK, the findings indicated that management capability may only be expressed through better management practice, that is, management of innovation, human resource management (HRM), R&D and human resource development quality. This study however, measured financial stability using management capability with proxies strategic planning corporate governance, audit programs, information system controls and human resource management.

Methodology

This study adopted research philosophy pursued by positivism and employed explanatory research design. This study used cross sectional survey to collect primary data from a total population of 704 respondents among 176 DT-SACCOs in Kenya. The study used a standard questionnaire to gather voluntary responses from each DT-SACCO; head of risk, head of Information Communication Technology and business innovations, finance manager and executive- SACCO board member within a sample size of 256 respondents. Stratified sampling was further adopted in selecting study participants who were reflected to be knowledgeable of the variables under study from year 2018 to 2023.Inferential and descriptive statistics (means, standard deviation, frequencies and percentages) were obtained using Statistical Package for the Social Sciences version 26 and findings presented in forms of table formats and graphs. Regression analysis was conducted for inferential statistics after diagnostic tests.

Results and Discussion

General Information

The study gathered primary data for data breach risk and financial stability from successful 217 participants providing a response rate of 84.8 percent out of 256 sampled respondents among DT-SACCOs in Kenya for a period of 5 years (2018 – 2023). Majority (58.1%) of the study respondents were male, while 41.9 % were female, indicating that the findings of this study are representative of both genders' perspectives. Findings reported that data breach risk and financial stability of DT-SACCOs in Kenya incorporated diverse ages, and thus the findings would be considered representative. 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 member. Further, results implied that the 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.

Descriptive Analysis of Variable Measure

Data was collected using a 5-point Likert scale for both data breach risk and financial stability where respondents were required to rate their level of agreement with statements on a scale of 5, with one representing strongly disagree and five representing strongly agree.

Adoption of 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
The board of directors and management of DT- SACCOs in Kenya maintain very 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 DT-SACCOs should ensure effective security information controls are in place to safeguard members' investments and data.	3.00	0.544
DT-SACCO employees should be thoroughly trained on specific daily operations to meet the needs of the firm so as to improve financial stability.	4.12	0.460
A robust strategic plan developed by board of directors and management can provide resilience to financial system hence strengthening financial stability of a DT-SACCO.	3.00	0.529
To ensure financial stability, DT-SACCOs audit programs should be independent, reported to the supervisory committee without conflict or interference from management.	3.02	0.504

Data Breach Risk and Financial Stability

This section covers the descriptive analysis of the primary data gathered in the study on the influence of data breach risk on financial stability of DT-SACCOs in Kenya. The measurements under data breach risk variable were hacking, insider threat and unpatched software's. Table 2 provides the summary statistics.

Table 2. Data Breach Risk and Financial Stability

Questionnaire Items for Data Breach Risk	Mean	Std. Deviation
Hacking		
By ensuing robust policies and procedures that address fundamental controls necessary to reduce the impact of hacking, DT-SACCOs in Kenya can positively affect their financial stability.	2.02	1.438
Employing relevant professional certified staff in information security service providence, enhance financial stability of a DT-SACCO.	2.11	1.385

DT-SACCOs use two-factor authentication or multi-factor authentication for both remote and internal administrative access to the broader banking network to ensure only authorized personnel can get access to internal systems fostering financial stability.	1.97	1.435
The use of high degree of security in storing and backing – up data enhances financial stability.	1.87	1.405
Insider Threat		
Allowing backdoors to access data remotely can negatively affect financial stability.	1.94	1.466
Active regulations imposed to cloud service providers for security systems to mitigate inside threat enhances financial stability.	2.05	1.274
Installation of non-approved software on network computers can cause attacks weakening the financial systems, therefore negatively impacting financial stability of DT-SACCOs.	1.92	1.427
Weak passwords and application programming interfaces exposes confidentiality thus having a negative influence on financial stability of DT-SACCOs.	1.94	1.465
DT- SACCO that view insider threat as a people problem, rather than the conventional technical approach experience a more stable financial system.	1.90	1.443
Unpatched Software		
DT-SACCOs that track vulnerability patches experience high financial stability.	1.96	1.409
Critical safety dependencies on each software update should be examined to identify its integration with the financial system.	1.83	1.457
All DT-SACCOs in Kenya enriched with a backup security patching to prevent attackers from exploiting existing vulnerabilities have a strong financial stable system.	1.79	1.431

Correlation Analysis

The Pearson correlation analysis was used to determine the strength and direction between data breach risk and financial stability as shown in Table 3. The results indicate a weak negative correlation between data breach risk and financial stability. The correlation coefficient is -0.113 and the p-value is less than 0.05, suggesting that this negative relationship is statistically significant ($r = -0.113$, $p = 0.048$, $p<0.05$). These findings imply that as data breach risk increases, there would be a decrease in financial stability and vice versa.

Table 3: Correlation Between Data Breach Risk and Financial Stability

		Data Breach Risk
Financial Stability	Pearson Correlation	-.113*
	Sig. (2-tailed)	.048
	N	217

*. Correlation is significant at the 0.05 level (1-tailed).

Regression Analysis

The research used ordinary least square regression analysis to test the relationship between data breach risk and financial stability of Deposit Taking SACCOs in Kenya. Diagnostic tests were conducted to confirm the suitability of the data for modelling. Findings indicated that the items used to measure the variable of data breach risk did not exhibit any substantial deviation from a normal distribution. None of the relationship tests had a variance inflation factor above 5, they ranged between 1.017 and 1.118 indicating that no multicollinearity existed between the measures.

Table 4: Coefficients

Model	Unstandardized B	Std. Error	Standardized Beta	t	Sig.
Constant	1.432	0.130		11.017	0.000
Data Breach Risk	-0.166	0.099	-0.113	-1.670	0.048

The findings in table 4 indicate that the model has predictive power and is significant. $P < .05$, explained that the coefficients are statistically significantly different to 0 (zero). The test states that data breach risk p (.048) <0.05 is significant. The findings reveal a negative and statistically significant influence of data breach risk toward financial stability of DT-SACCOs in Kenya at a 5 % significance level ($t = -1.670$, $p < 0.05$).

The model derived from the analysis was:

$$\textit{Financial Stability} = 1.432 - 0.166\ (\textit{Data Breach Risk}) + \varepsilon$$

The constant term 1.432, is the predicted value for the dependent variable (in this model) financial stability if independent variable, data breach risk = 0. That is, we would expect financial stability of 1.432 when predictor variable, data breach risk takes the value 0. The unstandardized coefficient for data breach risk is -0.166. This means for every unit increase in data breach risk, there is 0.166 decrease in financial stability.

Table 5: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.113[a]	0.013	0.008	0.63911

The correlation coefficient (R= 0.113) in this model, indicates a weak level of prediction. The standard error 0.63 of this model fit is a measure of the precision of the model. It represents the standard deviation of the residuals. Therefore, from the analysis, data breach risk has a weak negative correlation against financial stability and the Durbin Watson value of 1.741 indicates there is no autocorrelation since the value is between 1 and 3.

Table 6 ANOVA Results

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	1.139	1	1.139	2.789	0.048
Residual	87.820	215	0.408		
Total	88.960	216			

The F-ratio tests whether the overall regression model is a good fit for the data. The findings showed that the independent variable, data breach risk statistically significantly predicted the dependent variable, F (1, 215) = 2.789, p (.048) < .05. Therefore, the regression model is a good fit of the data and that data breach risk is significant in determining financial stability of DT-SACCOs in Kenya. The findings indicated that the influence of data breach risk was statistically significant in explaining changes in the Financial Stability of DT-SACCOs in Kenya, hence the ANOVA results was used to test the null hypothesis.

As a result, the null hypothesis,

H_0: There is no statistically significant Influence of Data breach risk on Financial Stability of Deposit Taking SACCOs in Kenya, was rejected and the alternative hypothesis was supported.

Discussion

The study examined the influence of data breach risk on financial stability of deposit taking SACCOs in Kenya. The study findings indicated that data breach risk had a negative statistically significant influence on financial stability. The findings were consistent with Jiaojiao (2022) who assessed the effect of data breaches in the financial service industry among top-listed United States financial institutions during a nine years' time frame 2010-2018. From the study, among 58 firms, there were 88 data breaches observations. The study findings concluded that data breach negatively significantly affect financial stability. However, study by Jiaojiao (2022) was conducted in form of secondary sources whilst the current study obtained primary sources of data. Moreover, Cansu, Erhan, Yigit and Muhittin (2021) studied financial impact of data breaches on financial firms in United states from the year 2001 to 2018. Data from 192 measures were analyzed by employing Event Study Methodology based on quantitative approach. Data was collected secondarily from technology portals, newspapers and the website of a nonprofit organization named Privacy Rights Clearinghouse. Findings indicated that financial firms' stability had a significant negative impact to data breaches consistent to the current study. The deviations of the findings can be due to methodological approach as the study was collected secondarily while the current study data was collected primarily.

From the study, data breach risk has negative significant influence on financial stability. However, the findings contradict with Lars and Morten (2019) who conducted a study on data breach and financial stability of 15 financial firms affected by data breaches from year 2006 to 2018 in Canada, China, France, United Kingdom, Switzerland, Japan and USA. Using qualitative case study, multiple variable regression was used to test the statistical significance level. Findings indicated that, investors value news of a data breach negatively, as a statistically significant market value loss is present instantly following the discovery of a data breach. This divergence could be due to difference in geographical context. The study by Lars and Morten

(2019) was conducted from year 2006 to 2018 in Canada, China, France, United Kingdom, Switzerland, Japan and USA while the current study was conducted in Kenya.

The findings also contradict with Jerotich, Silvance and Benard (2019) who examined data breaches and financial stability among SACCOS in Kenya. The study adopted simple random sampling to select 85 SACCOS. Purposive sampling was further used in selecting 85 information technology personnel participants. The study recognized that in all the SACCOS studied, data breach positively significantly affected financial stability. Despite the inconsistency in findings, some questions may be raised due to deviations on the sampling method and sampling size.

Conclusion

This study investigated the influence of data breach risk on financial stability of deposit taking SACCOs in Kenya. Findings suggest that data breach risk had a negative and significant influence on financial stability of DT-SACCOs in Kenya. Furthermore, the results indicated that data breach risk had a moderate negative correlation relationship with financial stability. Thus, the study rejected the null hypothesis and concluded that data breach risk has significant influence on Financial Stability of Deposit Taking SACCOs in Kenya.

Recommendations

To curb data breach risk, DT-SACCOs should track vulnerability patches, update Softwares and ensure enriched patching backup security. In view of this, it is recommended that management should impose active regulations to cloud service providers for security systems to mitigate insider threats. Further, installation of approved software on network computers and adequately tracking patches can lead to a more reliable financial system.

References

Abby, B. (2021). *The ins and outs of launching a digital savings product in Kenya: Regulatory guidance for fintech startups.* https: digital-savings-product Kenya regulatory guidance for FinTech.

Betz, L. (2016). *An analysis of the relationship between security information technology*

enhancements and computer security breaches and incidents. (ProQuest Dissertations & Theses Global).https://search.proquest.com/dissertations-theses/analysis-relationship-between-security/docview/1786673242/se-2? accountid=10378

Cansu, T., Erhan, A., Yigit, K., & Muhittin, S. (2021). The financial impacts of information systems security breaches on publicly traded companies: reactions of different sectors. *Journal of Enterprise Information Management,* 1741-0398. https://www.emerald.com/insight/1741-0398.htm

Console, R. (2022). *First financial credit union confirms data breach resulted in leaked member data.* Personal Injury Updates publishers.

David, H.P. (1997). *Bank risk management theory. research program in finance working papers RPF-272.* University of California at Berkeley.

FinAccess (2021). *Financial inclusion in Kenya.* International Monetary Fund

Gai, K., Qiu, M., & Sun, X. (2018). A survey on FinTech. *Journal of Network and Computer Applications, 103*, 262–273.

Gurley, J.G., & Shaw, E.S. (1960). *Money in a theory of finance*. Brookings.

Jerotich, S., Silvance, O. A., & Benard, O. (2019). Assessing the Current Status of Information Security Policies among Saccos in Kenya. *European Journal of Business and Management,* 11 (27), 2222-1905.

Jiaojiao, F. (2022). *The effect of data breaches in the financial service industry: an empirical study.* (Dissertation, Hong Kong Polytechnic University). https://theses.lib.polyu.edu.hk/handle/200/12172

Lars T. S., & Morten, R. (2019). *The financial implications of a data breach and how to manage the crisis.* (Master's Thesis).

Manju, B., Senbagavalli, M., Ejashvar.K.R., & Tejashwini, K.R. (2022). Data Breach – Its Effects on Industry. *International Journal of Data Informatics and Intelligent Computing, 1*(2),51-57.

Nzuva, S. (2019). Enhancing data breach risk management: a case study of Kenyan Commercial Banks. *International Journal of Engineering Trends and Technology, 67*(10).

Penny Tamkin, Jim Hillage, Rebecca W. (2002). indicators of management capability: developing a framework. *The Institute for Employment Studies Privacy Rights Clearinghouse*. (2018, February 2). Data Breaches. From Privacy Rights Clearingshouse: https://www.privacyrights.org/data-breaches

Rashed, J. (2019). *Peer to peer (p2p) lending.* (Istanbul Sabahattin Zaim University).

Roy, U. (2021). *Data breaches: A resurging threat for credit unions and members.*

SASRA (2019). *The Sacco Societies Regulatory Authority (SASRA).* Supervision Report. Nairobi, Kenya.

SASRA. (2023). *The SACCO supervision annual report, 2020.* The Annual Statutory Report on the operations and performance of SACCO.

Yu, P. (2021). *Risk management theory explained*.https://www.iienstitu.com/en/blog/risk-management-theory-explained.