Int Journal of Social Sciences Management and Entrepreneurship 8(1): 956-969 2024

ISSN 2411-7323

www.sagepublishers.com

CYBERSECURITY AND PERFORMANCE OF INTERNET BANKING SERVICES IN COMMERCIAL BANKS IN NAIROBI CITY COUNTY, KENYA

[1] Samoei Pamela Cherotich, [2] Dr. Gatobu Purity

[1] MsC Student ICT Management, Jomo Kenyatta University of Agriculture and Technology

[1] Lecturer, Jomo Kenyatta University of Agriculture and Technology

ABSTRACT

The commercial banks globally and locally have adopted technology in carrying out banking transactions. Technology helps reduce the costs of administration and operation as well as increasing convenience in banking. However, even with the immense perceived benefits of the use of technology in banking, internet banking has been faced with challenges including fraud and loss of funds. The major challenge that comes with increased adoption of technology in the banking services is cybercrime. This study therefore aims at determining the impact of cybersecurity on the performance of internet banking services of commercial banks in Nairobi City County. The study adopted a descriptive research design with a census of a target population of 38 licensed commercial banks in Nairobi City County. The study used primary data that was collected using a structured questionnaire. The data was then analysed using the Statistical Software for Social Sciences (SPSS) and the results presented in the form of tables. The study concluded that application security is a significant determinant of the performance of internet banking services. IT governance is a significant determinant of the performance of internet banking services. The study recommends that the commercial banks ought to enhance the security of their mobile banking apps to protect customer information and funds from cyber attackers. This includes adding more person-specific security features that may include the use of fingerprints and 2FA codes. The commercial banks further ought to enhance IT governance that may be done by a professional and dedicated team to enhance the level of trust and customer satisfaction as well as competitiveness.

Key Words: Cybersecurity, Internet Banking Services, Commercial Banks, Application Security, IT Governance

Background of the Study

Technology has been incorporated by businesses globally in the provision of goods and services. Technology is currently considered as the major contributing factor towards the success of most firms that have incorporated it (Tsou & Chen, 2022). The banking industry has adopted technology in its operations and management because of the need to reduce the costs of administration and operations. This is by the introduction of electronic and mobile banking services which are accessible easily and conveniently to its customers (Kenya, 2019).

Internet banking entails a system whereby the customers of a particular financial institution conduct their financial transactions electronically. Through internet banking, the customer is able access banking services electronically without visiting the bank (Arshad Khan & Alhumoudi, 2022). Internet banking refers to the systems that customers use to assess accounts, obtain financial information regarding products and services and transact business through a public or private network, including the internet (Khan, 2017). The internet banking services include online banking, phone banking, mobile banking, ATM and debit card services, fund transfers, e-statements among others (Boni & Tsekeris, 2007). Internet banking can also be used to make remittances both local and international. Internet banking is preferred because it is less costly.

Internet banking entails an electronic payment system that makes it possible for the commercial bank customers to carry out various financial transactions online through the internet. The customers can access various bank products conveniently at the convenience of their location any time provided there is network coverage (Jahan et al., 2020). Furthermore, the other motivational factor that may have compelled the commercial banks to adopt internet banking services is the widening of the revenue base as well as for growing profits. With internet banking, the banks have recorded increased transactions and increased convenience of transactions and hence increased revenues (Odhiambo & Ngaba, 2019).

However, even with the advent of internet banking that has been widely adopted by the commercial banks, a number of security issues have been of concern to the customers globally (Ghorbani & Ahmadzadegan, 2017). Internet banking exposes customers to fraud, theft and other related security issues, which may be attributed to customer behaviour when carrying out transactions on the platforms. The major challenge that comes with increased adoption of technology in the banking services is cybercrime. Thus, this calls for proper security when designing online banking systems to mitigate security attacks and fund losses due to security vulnerabilities (Ameme & Yeboah-Boateng, 2016).

Cybersecurity entails the involvement of policies, people, processes and technologies to protect the organizations and their systems from the digital attacks (Khalil, *et al.*, 2020). It is the process designed to protect the servers, computers, networks and digital data from unauthorized access and destruction or attack in cyberspace. This covers the protection of financial data and the business reputation (Al-Alawi & Al-Bassam, 2020). The technological advancement has resulted in cybersecurity challenges and there is need for the governments and institutions to up the legal and technical frameworks to curb the challenge (Uddin, *et al.*, 2020).

Cyber security threats have more affected financial related institutions, commercial organisation and government agencies. The commercial banks and other financial institutions hold sensitive information especially the financial information of its customers (Belás, et al., 2016). The internet banking system has been a target by criminals and hackers whose main intentions are to steal the financial information of clients and the funds (Ali, *et al.*, 2020). The commercial banks must therefore, be up to date with new technological trends to protect the data of their clients (Al-Alawi & Al-Bassam, 2020). Even though most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to

damage or disable them, while others use computers or networks to spread malware and illegal information among others (Jethwani & Surbhi, 2015).

Statement of the Problem

There has been stiff competition among the Kenyan commercial banks each intending to remain competitive in the Kenyan financial market. As a result, the banks have focused on incorporating technology in their operations to enhance service delivery to its customers and remain competitive (Njoroge & Mugambi, 2018). Many commercial banks have appreciated that an increasing number of customers prefer consuming banking services electronically. The banks have also began offering 24-hour banking services to its customers because of the increased convenience of service access (Amin, 2016). Through internet banking, banking services are efficient and safe. The commercial banks are able to manage employees, expand their markets, attain consumer competitiveness and achieve consumer loyalty (Nduta & Wanjira, 2019).

However, despite the advantages of using internet banking, the system is susceptible to fraud, overload, security & privacy problems, rapid technology change, high initially cost and uncertainly about information reliability (Daniela et al, 2010). The commercial banks and other financial institutions hold sensitive information especially the financial information of its customers. This sensitive information is a subject of interest to the cybercriminals who hold specialised information technology skills. They capitalise on the loopholes that may exist within the banking security system to try to access customer information.

The internet banking system has been a target by criminals and hackers whose main intentions are steal the financial information of clients and the funds. Cyber-attacks in Kenya have been on the rise in the banking and financial sector according to the Kaspersky report (2021). The cyber-attacks increased from the first quarter of 2021 to the second 2021 by 59% and the main leading cyber security threats are crypto-miner malware, financial Trojans and ransomware. An estimated KES 18 billion was lost to cybercrime in 2016 (Kenya National Bureau of Statistics, 2016). The proposed study seeks to determine the impact of cybersecurity on the performance internet banking services of commercial banks in Nairobi City County.

A number of studies have been conducted on cyber insecurity and its impact on the socioeconomic, cultural and political dimensions of the society (Gandhi, et al., 2011; Dunn Cavelty & Wenger, 2020; Apaua and Lallie, 2022). Though the studies established that cybersecurity has adversely impacted the cultural, social, economic, and political dimensions, the manifestations of cyber insecurity is very dynamic and rapidly evolving. With these rapid changes and dynamic of cyber security, the practicality, policy framework and scholarly implications relating to cyber security a decade ago may not be applicable and practical now and in the future. As such, continuous research on cyber insecurity is critical to identify new dynamics that cyber insecurity drives, with particular attention to end users, system and application security, IT governance and IT infrastructure. A study by Apaua and Lallie, (2022), Chang, (2016), He et al. (2015) and Islam, (2014) did not clearly capture the application and end-user security regarding the mobile banking applications, a gap the current study seeks to fill. In addition, Das and Dhar (2014), Belás et al. (2016), Awwad and El Khoury, (2021) and Alansari, Huang et al. (2011) and Al-Sartawi, (2021) in their studies on IT governance did not capture the effect of IT governance on the performance of internet banking services among the Kenyan commercial banks, a gap that is sought to be filled by the current study. Finally, Sarjiyus et al. (2019) and Rajarajeswari et al. (2021) in their studies did not bring out clearly the effect of IT infrastructure on the performance of internet banking services among the Kenyan commercial banks. The current study seeks to fill this gap. It is against this that the proposed study seeks to determine the impact of cybersecurity on the performance of internet banking services of commercial banks in Nairobi City County.

Objectives of the Study

The specific objectives were,

i. To establish the effect of application security on the performance of internet banking services of commercial banks in Nairobi City County.
ii. To analyze the effect of IT governance on the performance of internet banking services among commercial banks in Nairobi City County.

LITERARTURE REVIEW

Theoretical Review

Theory of Reasoned Action

The theory of reasoned action was formulated by Fishbein and Azjen in 1967. The theory postulates that the behaviour of a person is determined by their intention to perform that behaviour. The intention is a function of their attitude towards the behaviour and subjective norms (Kim et al., 2013). The attitude towards performing a particular action is determined by the likelihood of various consequences as well as the evaluation of the impact of such consequence if any. In case of a feeling that the consequence would be good or beneficial, then the action is deemed necessary. On the other hand, if the consequences are deemed to be dire and negative, then the actioned would be deemed unnecessary of non-beneficial to perform (Trafimow, 2009).

The theory of reasoned action has however been criticised by a number of scholars. One of the criticism against the theory is that the theory is not falsifiable. The theory makes risky predictions that can only be falsified under reasonable standards of falsification. The theory further has a significant risk of confounding between attitudes and norms. This is because attitudes mostly can be reframed as norms and that norms can be reframed as attitudes. Therefore, this confusion has been considered as one of the limitations of the theory (Hagger, 2019).

The theory is relevant to the study on the impact of cybersecurity on the performance of internet banking services of commercial banks in Nairobi City County. This because the incidences of cyber-attacks are considered as actions that are well thought by the cyber criminals with the intention of reaping benefits from the act. The cyber criminals are also aware of the consequences of the action and the behaviour of the commercial banks and its customers. Thus, the theory can be used to explain the study.

Technology Acceptance Theory

Technology acceptance model theory was postulated by Fred Davis in 1989. The theory points out that the acceptance of a computer system by its potential users depends on two main factors that is the perceived ease of use and the perceived usefulness. The theory thus drives on the perceptions of the users of the computer systems (Granić & Marangunić, 2019). The theory is an improvement of the theory of reasoned action. The theory of reason action is grounded on the fact that believes influence attitudes leading to intentions, which ultimately generate behaviour. Davis, (1989) introduced added the perceived usefulness, perceived ease of use, attitude and behavioural intention to use which would lead to the system usage (Ma, & Liu, 2004).

The theory has been criticised in that the variable pertaining to the user behaviour evaluated through a subjective means such behavioural intention and interpersonal influence. In addition, behaviour cannot be expressly quantified owing to a number of different subjective factors such as the values and norms of societies and personal attributes and personality traits. Hence, the

argument that a relative, friends could influence the use of technology through exacting social pressure is highly falsifiable (Ajibade, 2018).

The theory is relevant to the current study because cybersecurity is highly dependent on technology and the use of technological devices. The cyber criminals use devices such as computers in the execution of cyber-attacks. This could be because of the perceived ease of use and the perceived usefulness of the technological systems. Thus, the theory was significant in giving explanations on cybersecurity and its effect on internet banking services of commercial banks in Nairobi City County.

Conceptual Framework

A conceptual framework presents a pictorial representation of how the dependent and the independent variables in a research are expected to relate. The dependent variable in this study is the performance of internet banking services of the commercial banks in Nairobi City County. The independent variables on the other hand include, the application security, and IT governance. It is expected that the application security, and IT governance had an impact on the performance of internet banking services of the commercial banks in Nairobi City County. A summary of the expected relationship between the variables is summarized in Figure 2.1.

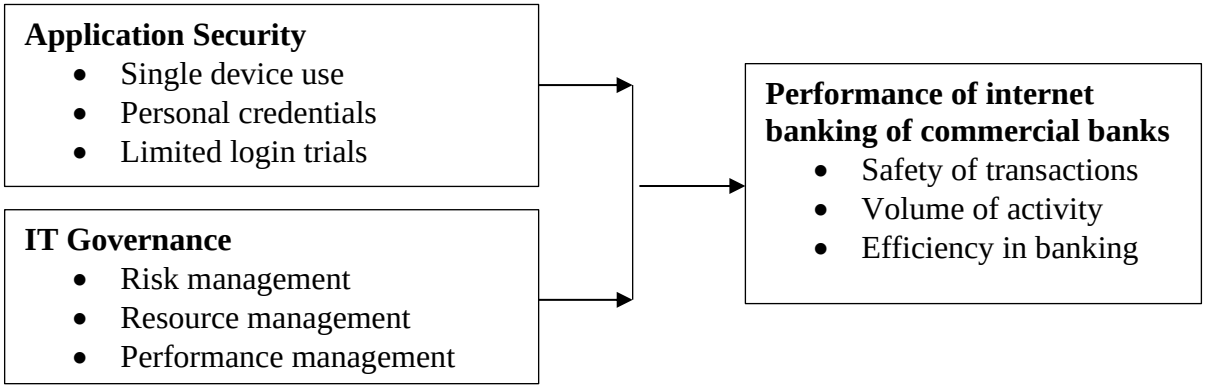

Figure 2.1: Conceptual Framework

Application Security

Application security pertains the inherent risks and security vulnerabilities in the mobile banking apps (Kouraogo et al., 2017). The risks may include unsecured server communication and data storage, vulnerabilities in the code, failure to authenticate certificates, and running on phones despite the phones being broken. Some applications were found to be initiating non-encrypted connections, did not validate the authenticity of certificates from the server, and some of them being accessible through a web interface that made the phones more vulnerable to JavaScript injections seeking to steal login information (Chang, 2016). Sarjiyus et al. (2019) pointed out that banks should have security measures in place including include protecting customer confidential information to protect clients from phishing, trojans and other viruses, avoiding public networks, which a source of attacks such as spoofing, phishing, pharming and keystroke capturing.

IT Governance

IT governance according to Webb et al. (2006) entail the process that ensures efficient and effective use of IT in enabling an organization achieve its objectives and goals. Information technology has enhanced the activities in the banking sector. The banking services are now available throughout at the convenience of the customers. Through IT, competition among the

banks has increased which has resulted in better systems and increased performance (Alansari & Al-Sartawi, 2021). Information technology can be applied in the banking system to facilitate the automated environment on which banking data is based, enhance the distribution and delivery channels of the banks, develop new services and products to remain competitive in the financial markets, create a strategic resource as well as improving the payment system and monitoring transactions (Awwad & El Khoury, 2021).

Empirical Review

Application Security and Performance of Internet Banking Services

A study was conducted by Apaua and Lallie, (2022) in Ghana, focusing on measuring user perceived security of mobile banking applications. The study adopted a covariance-based structural equation modelling with a total of 315 responses used in analysis. The results pointed out that the advent of mobile banking has triggered the rapid increase in the mobile banking financial web apps. The apps are beneficial in that they are easy to use and offer comfort when performing financial transactions. However, despite the perceived benefits, there are inherent risks and security vulnerabilities in the mobile banking apps. The increase in the mobile applications have resulted in a corresponding increase in the appetite of cybercriminals and computer hackers to target such devices.

Chang, (2016) conducted a study on mobile banking with a focus on the best hope for cyber security development. The study indicated that most of the mobile banking applications are vulnerable to cyber-attacks and do not have the necessary security measures of protecting sensitive information. The results further pointed out that the apps faced unsecured server communication and data storage, vulnerabilities in the code, failure to authenticate certificates, and running on phones despite the phones being broken. Some applications were found to be initiating non-encrypted connections, did not validate the authenticity of certificates from the server, and some of them were accessible through a web interface that made the phones more vulnerable to JavaScript injections seeking to steal login information.

A research was conducted by He et al. (2015) with a focus on understanding mobile banking applications' security risks through blog mining and the workflow technology. Blog mining research method was adopted by the study. The findings pointed out the key security risks facing the mobile banking applications. According to the study, mobile malware is fast spreading and has caused a variety of security and privacy concerns including leaking of sensitive financial data, financial loss and identify theft. Thus, information on the emerging vulnerabilities, threats and the respective counter measures is necessary to the future of mobile banking and mobile banking users' financial security.

IT Governance and Performance of Internet Banking Services

Furthermore, Awwad and El Khoury (2021) while researching on information technology governance and bank performance in Palestine pointed out that information technology can be applied in the banking system to facilitate the automated environment on which banking data is based. Information technology also enhances the distribution and delivery channels of the banks, develop new services and products to remain competitive in the financial markets, create a strategic resource as well as improving the payment system and monitoring transactions. However, the banks have not been able to reap maximum benefits from the adoption of information technology. The banking sector still faces security threats as well as ineffective IT decision making and management control.

Focusing on IT governance and E-banking among the Gulf Cooperation Council listed banks, Alansari and Al-Sartawi (2021) indicated that banks and other financial institutions would achieve

effective operations when they adopt the information technology governance. The study acknowledged the role information technology has played in enhancing the activities in the banking sector. The banking services are now available throughout at the convenience of the customers. Through IT, competition among the banks has increased which has resulted in better systems and increased performance.

In a study on IT governance focusing on objectives and assurances in internet banking, Huang et al. (2011) established that the commercial bank customers have been reluctant in adopting internet banking as a result of the associated security issues. Customers have been able to associate every bank with its respective quality of services and their perceived security of carrying out transactions within their platforms. The quality internet banking according to the study has a positive impact on customer satisfaction. Internet banking can be employed to reduce system-related uncertainty by utilizing encrypted transactions, firewalls, authentication mechanisms, and privacy seals and disclosures. Furthermore, information technology can be used in routine transactions including efficient and effective control, allocation, and management of various IT service operations.

RESEARCH METHODOLOGY

This research adopted a descriptive research design. The unit of analysis of the study were the 38 licensed commercial banks that are operating in, Nairobi City County, Kenya. The commercial banks have been chosen because the cyber security threats mostly target commercial banks and other financial institutions. The unit of observation of the study were 38 IT administrators, 38 network administrators and 38 database administrators selected from each of the 38 licensed commercial banks that are operating in, Nairobi City County. Thus, the target population for the study were 114 respondents. Since the target population in this research is relatively small, a census of all the 38 IT administrators, 38 network administrators and 38 database administrators of all the 38 licensed commercial banks in Nairobi City County The study used primary data for analysis. A structured questionnaire was used to collect data from the respondents. The data from the questionnaires were transferred to an excel sheet after which the data was loaded to SPSS for analysis. The results were presented in the form of descriptive and inferential results. The descriptive statistics comprised percentages, means and standard deviation. The inferential statistics comprised the Pearson's correlation coefficient (r) and multiple linear regression model.

RESULTS AND DISCUSSION

Studies including a study by Fincham (2008) have indicated that good response rate in research studies should have a response rate of at least 70%. The sample size for the study was 114 respondents. 8 respondents participated in the pilot study. Thus, 106 respondents participated in the main study.

Application Security

The study adopted primary data that was collected using structured questionnaires administered to the respondents. The questionnaires were structured in a Likert scale from points 1 to 5 whereby point 1 represented Not at all, 2 for Small extent, 3 for Moderate extent, 4 for Great extent and 5 for Very great extent. In the analysis of data, the descriptive statistics were presented in the form of frequencies, means and standard deviation as well as percentages. A mean of 1 indicated that on average, the responses strongly disagreed with the respective statement presented, a mean of 2 indicating an agreement to small extent, mean of 3 an agreement to a moderate extent, a mean of 4 an agreement to a great extent and finally a mean of 5 indicating an agreement to a very large extent. Table 1 presents a summary of the responses with regards the questions on application security.

Table 4.3: Descriptive Results for Application Security

	NAA	SE	ME	GE	VGE		
	f %	f %	f %	f %	f %	M	S Dev
Linking credentials of the app to those of the bank account helps enhance performance of e banking	1 1.1%	14 15.1%	17 18.3%	32 34.4%	29 31.2%	3.8	1.1
Limiting the daily amounts to be transacted is a good security measure to boost performance of e banking.	1 1.1%	11 11.8%	18 19.4%	32 34.4%	31 33.3%	3.9	1.0
Limiting the number of login trials helps improve performance of e banking	3 3.2%	11 11.8%	24 25.8%	25 26.9%	30 32.3%	3.7	1.1
Limiting the ability to re-install the app and successfully login in a different device is an essential security step	3 3.2%	13 14%	15 16.1%	39 41.9%	23 24.7%	3.7	1.1
Enabling two-factor authentication is necessary in ensuring performance of e banking	3 3.2%	14 15.1%	9 9.7%	40 43%	27 29%	3.8	1.1

It can be noted from the responses in Table 4.3 that 32(34.4%) of the respondents agreed to a great extent that linking credentials of the app to those of the bank account helps enhance performance of e banking with 29(31.2%) concurring to a very great extent. However, 17(18.3%) agreed to a moderate extent. The statement mean and standard deviation were 3.8 and 1.1 respectively indicating that on average, the responses were in tandem to a great extent with the question.

The statement, limiting the daily amounts to be transacted is a good security measure to boost performance of e banking recorded responses as follows. 18(19.4%) of the responses were moderately in agreement, 32(34.4%) concurred to a great extent, 31(33.3%) of the responses were in tandem to a very great extent. The mean and the corresponding standard deviation of the statement were 3.9 and 1.0 respectively implying that the respondents agreed to a great extent with the question.

Limiting the number of login trials helps improve performance of e banking attracted responses as follows. 25(26.9%) of the respondents agreed to a great extent, 30(32.3%) concurring to a very great extent. However, 24(25.8%) agreed to a moderate extent. The statement mean and standard deviation were 3.7 and 1.1 in that order indicating that on average, the responses were in tandem to a great extent with the question.

In addition, the responses regarding the question, limiting the ability to re-install the app and successfully login in a different device is an essential security step pointed out the following. 39(41.9%) of the respondents were in agreement to a great extent, 15(16.1%) agreed to a moderate extent whereas 23(24.7%) indicated an agreement to a very great extent. The mean and the standard deviation of the statement were 3.7 and 1.1 in that order meaning that the responses were in agreement to a great extent on average.

Finally, on whether enabling two-factor authentication is necessary in ensuring performance of e banking, 40(43%) of the responses were in tandem, 27(29%) indicated an agreement to a moderate extent and 27(29%) indicating concurrence to a very great extent. The mean and the standard deviation of the statement were 3.8 and 1.1 in that order meaning that the responses were in agreement to a great extent on average.

IT Governance

The responses regarding the questions on IT Governance are summarized in Table 2.

Table 2: Descriptive Results for IT Governance

	NAA	SE	ME	GE	VGE		
	f %	f %	f %	f %	f %	M	S Dev
Regular app maintenance is a significant security measure in enhancement of performance of e banking	2 2.2%	12 12.9%	14 15.1%	35 37.6%	30 32.3%	3.8	1.1
The presence of a reliable customer support helps boosting the performance of e banking	1 1.1%	11 11.8%	20 21.5%	38 40.9%	23 24.7%	3.8	1.0
Blocking suspicious customer app logins enhances the performance of e banking	3 3.2%	10 10.8%	16 17.2%	39 41.9%	25 26.9%	3.8	1.1
Flagging off transactions is useful in realising the performance of e banking	3 3.2%	11 11.8%	17 18.3%	29 31.2%	33 35.5%	3.8	1.1
Regular account transaction monitoring is key in ensuring performance of e banking	1 1.1%	11 11.8%	18 19.4%	36 38.7%	27 29%	3.8	1.0

From the results in Table 2 that 35(37.6%) of the respondents agreed to a great extent that regular app maintenance is a significant security measure in enhancement of performance of e banking with 30(32.3%) concurring to a very great extent. Additionally, 14(15.1%) agreed to a moderate extent. The statement mean and standard deviation were 3.8 and 1.1 respectively indicating that on average, the responses were in tandem to a great extent with the question.

The question, the presence of a reliable customer support helps boosting the performance of e banking recorded responses as follows. 20(21.5%) of the responses were moderately in agreement, 38(40.9%) concurred to a great extent, 23(24.7%) of the responses were in tandem to a very great extent. The mean and the corresponding standard deviation of the statement were 3.8 and 1.0 respectively implying that the respondents agreed to a great extent with the question.

Blocking suspicious customer app logins enhances the performance of e banking attracted responses as follows. 39(41.9%) of the respondents agreed to a great extent, 25(26.9%) concurring to a very great extent. However, 16(17.2%) agreed to a moderate extent. The statement mean and standard deviation were 3.8 and 1.1 in that order indicating that on average, the responses were in tandem to a great extent with the question.

In addition, the responses with regards to the question, flagging off transactions is useful in realising the performance of e banking pointed out the following. 29(31.2%) of the respondents were in agreement to a great extent, 17(18.3%) agreed to a moderate extent whereas 33(35.5%) indicated an agreement to a very great extent. The mean and the standard deviation of the statement were 3.8 and 1.1 in that order meaning that the responses were in agreement to a great extent on average.

On whether regular account transaction monitoring is key in ensuring performance of e banking, 36(38.7%) of the responses were in tandem, 18(19.4%) indicated an agreement to a moderate extent and 27(29%) indicating concurrence to a very great extent. The mean and the standard

deviation of the statement were 3.8 and 1.1 in that order meaning that the responses were in agreement to a great extent on average.

Performance of Internet Banking Services

The responses regarding the questions on performance of internet banking services are summarized in Table 3.

Table 3: Descriptive Results for Performance

	NAA	SE	ME	GE	VGE		
	f %	f %	f %	f %	f %	M	S Dev
Internet banking has led to increased volume daily transactions	2 2.2%	11 11.8%	23 24.7%	30 32.3%	27 29%	3.7	1.1
Internet banking has increased the efficiency in banking	2 2.2%	10 10.8%	20 21.5%	38 40.9%	23 24.7%	3.8	1.0
Internet banking has improved the competitive advantage of the bank	3 3.2%	12 12.9%	17 18.3%	36 38.7%	25 26.9%	3.7	1.1
Internet banking has boosted the revenue generation of the bank	2 2.2%	16 17.2%	17 18.3%	29 31.2%	29 31.2%	3.7	1.1
With internet banking, there is increased safety of financial transactions.	0 0%	11 11.8%	24 25.8%	32 34.4%	26 28%	3.8	1.0

On whether internet banking has led to increased volume daily transactions, 30(32.3%) of the responses were in tandem, 23(24.7%) indicated an agreement to a moderate extent and 27(29%) indicating concurrence to a very great extent. The mean and the standard deviation of the statement were 3.7 and 1.1 in that order meaning that the responses were in agreement to a great extent on average.

The responses with regards to the statement, internet banking has increased the efficiency in banking pointed out the following. 38(40.9%) of the respondents were in concurrence to a great extent, 20(21.5%) agreed to a moderate extent whereas 23(24.7%) indicated an agreement to a very great extent. The mean and the standard deviation of the statement were 3.8 and 1.0 in that order meaning that the responses were in agreement to a great extent on average.

The statement, internet banking has improved the competitive advantage of the bank, recorded responses as follows. 17(18.3%) of the responses were moderately in tandem, 36(38.7%) concurred to a great extent, 25(26.9%) of the responses were in tandem to a very great extent. The mean and the corresponding standard deviation of the statement were 3.7 and 1.1 in that order implying that the respondents agreed to a great extent with the question.

Internet banking has boosted the revenue generation of the bank attracted responses as follows. 29(31.2%) of the respondents agreed to a great extent, 29(31.2%) concurring to a very great extent. However, 17(18.3%) agreed to a moderate extent. The statement mean and standard deviation were 3.7 and 1.1 in that order indicating that on average, the responses were in tandem to a great extent with the question.

Finally, the statement, with internet banking, there is increased safety of financial transactions recorded the responses as follows. 32(34.4%) of the respondents were in agreement to a great extent, 26(28%) concurred to a very great extent. Additionally, 24(25.8%) agreed to a moderate

extent. The statement mean and standard deviation were 3.8 and 1.0 respectively indicating that on average, the responses were in tandem to a great extent with the question.

Correlation Results

Correlation analysis on the other hand is important in determining the strength and direction of relationship between the dependent and the respective independent variables. The dependent variable in the study was the performance of internet banking services whereas the independent variables included application security and It governance

Table 4: Correlation Results

		Performance of internet banking services	Application Security	IT Governance
Performance of internet banking services	Pearson Correlation	1		
	Sig. (2-tailed)			
	N	93		
Application Security	Pearson Correlation	.560**	1	
	Sig. (2-tailed)	0.000		
	N	93	93	
IT Governance	Pearson Correlation	.556**	.387**	1
	Sig. (2-tailed)	0.000	0.000	
	N	93	93	93

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

As can be observed from the results in Table 4, the correlation between the performance of internet banking services and application security was both positive and statistically significant ($r = 0.560$, $p = 0.000<0.05$). The correlation between the performance and IT governance was both positive and statistically significant ($r = 0.556$, $p = 0.000<0.05$).

Regression Results

Regression analysis is significant in determining the linear relationship between the dependent and the independent variables. The dependent variable in the study was the performance of internet banking services whereas the independent variables included application security and It governance

Table 5: Model Summary

R	R Square	Adjusted R Square	Std. Error of the Estimate
.740a	0.547	0.526	0.49577

a Predictors: (Constant), Application Security, IT Governance

It is clear from the results in Table 5 that the estimated model explains to a tune of 54.7% of the total variations in the performance of internet banking services. This is supported by the R Squared value of 0.547 in the estimated model. This implies that the independent variables under study are significant in explaining the performance of internet banking services.

Table 6: ANOVA

	Sum of Squares	df	Mean Square	F	Sig.
Regression	26.104	4	6.526	26.552	.000b
Residual	21.629	88	0.246		
Total	47.733	92			

a Dependent Variable: Performance
b Predictors: (Constant), Application Security, IT Governance

The results presented in Table 6 points out the statistical significance of the estimated model. This is supported by the estimated P value in the model (0.000<0.05) as well as the estimated F value (26.552) less than the F critical 1.99230 in the F tables. The estimated results can therefore be used to give reliable inference.

Regression Coefficients

The dependent variable in the study was the performance of internet banking services whereas the independent variables included application security, and It governance. Table 7 outlines the regression coefficient results.

Table 7: Regression Coefficients

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	-1.616	0.519		-3.115	0.002
Application Security	0.366	0.102	0.296	3.589	0.001
IT Governance	0.364	0.109	0.277	3.337	0.001

a Dependent Variable: Performance of internet banking services

The estimated multiple regression model was,

$$\mathbf{Y= -1.616 + .366X_1 + .364X_2}$$

Where

Y is performance of internet banking services of commercial banks in Nairobi City County

X_1 is application security,

X_2 is IT governance and,

It can be noted from the analysis regression coefficient results presented in Table 4.14 that, the coefficient of the variable application security was both positive (0.366) and statistically significant (p = 0.001<0.05). This implies that, a unit improvement in the security of applications would result in 0.366 units improvement in the performance of internet banking services among the commercial banks in Nairobi County. Thus, the study concludes that application security is a significant determinant of the performance of internet banking services.

The coefficient of the variable IT governance was both positive (0.364) and statistically significant (p = 0.001<0.05). This implies that, a unit improvement in IT governance would result in 0.364 units improvement in the performance of internet banking services among the commercial banks in Nairobi County. Thus, the study concludes that IT governance is a significant determinant of the performance of internet banking services.

Conclusions

The study concluded that application security is a significant determinant of the performance of internet banking services. Application security pertains the inherent risks and security vulnerabilities in the mobile banking apps including unsecured server communication and data storage, vulnerabilities in the code, failure to authenticate certificates, and running on phones despite the phones being broken. The utilization of technology in banking has resulted in an increase in mobile banking financial web apps, which are beneficial in that they are easy to use, and offer comfort when performing financial transactions. However, this has also resulted in a corresponding increase in the appetite of cybercriminals and computer hackers to target such devices. Most of the mobile banking applications are vulnerable to cyber-attacks and could cause a variety of security and privacy concerns including leaking of sensitive financial data, financial loss and identify theft. Thus, banks should have security measures in place including include protecting customer confidential information to protect clients from the security threats.

The study concluded that the study concludes that IT governance is a significant determinant of the performance of internet banking services. IT governance entail the process that ensures efficient and effective use of IT in enabling an organization achieve its objectives and goals. Information technology has been utilized in the banking system to facilitate the automated environment on which banking data is based. It enhances the distribution and delivery channels of the banks, develop new services and products to remain competitive in the financial markets, create a strategic resource as well as improving the payment system and monitoring transactions. Banks would achieve effective operations when they adopt the IT governance. Through IT, competition among the banks has increased which has resulted in better systems and increased performance. The quality internet banking according to the study has a positive impact on customer satisfaction.

Recommendations to Practice

The study recommends that the commercial banks ought to enhance the security of their mobile banking apps to protect customer information and funds from cyber attackers. This includes adding more person-specific security features that may include the use of fingerprints and 2FA codes. Furthermore, there should be adequate and regular training for the customers utilizing internet banking on the safety tips of utilizing the platform as well as the signs of cyber threats. This can be done through popular online platforms. The commercial banks further ought to enhance IT governance that may be done by a professional and dedicated team to enhance the level of trust and customer satisfaction as well as competitiveness. The commercial banks further ought to introduce more security measures including the use of fingerprints as well as timely notifications when customers are utilizing internet banking service.

Policy Recommendations

The study recommends that the ministry of Information, Communication and Digital Economy as well the Communications Authority of Kenya should regulate the mobile apps in place to ensure that they are safe for use by the various commercial bank customers. The commercial banks should also develop policies making it mandatory for the regular update and improvement of the apps to match the dynamic challenges.

Recommendations for Further Studies

The study recommends that further studies be conducted on internet banking and financial performance of microfinance institutions in Nairobi City County.

REFERENCES

Ajibade, P. (2018). Technology acceptance model limitations and criticisms: Exploring the practical applications and use in technology-related studies, mixed-method, and qualitative researches. *Library Philosophy and Practice*, *9*.

Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector. *Journal of Xidian University*, *14*(7), 1523-1536.

Alansari, Y., & Al-Sartawi, A. M. M. (2021). IT governance and E-banking in GCC listed banks. *Procedia Computer Science*, *183*, 844-848.

Ali, O. A. M., Matarneh, A. J., Almalkawi, A., & Mohamed, H. (2020). The impact of cyber governance in reducing the risk of cloud accounting in Jordanian commercial banks-from the perspective of Jordanian auditing firms. *Modern Applied Science*, *14*(3), 75-89.

Amin, M. (2016). Internet banking service quality and its implication on e-customer satisfaction and e-customer loyalty. *International Journal of Bank Marketing, 34(3), 280-306.*

Apaua, R., & Lallie, H. S. (2022). Measuring User Perceived Security of Mobile Banking Applications. *arXiv preprint arXiv:2201.03052*.

Arshad Khan, M., & Alhumoudi, H. A. (2022). Performance of E-banking and the mediating effect of customer satisfaction: a structural equation model approach. *Sustainability*, *14*(12), 7224.

Awwad, B., & El Khoury, R. (2021). Information technology governance and bank performance: Evidence from Palestine. *Journal of decision systems*, 1-24.

Belás, J., Korauš, M., Kombo, F., & Korauš, A. (2016). Electronic banking security and customer satisfaction in commercial banks. *Journal of security and sustainability issues*.

Boni, K., & Tsekeris, C. (2007). Electronic Banking. *The Blackwell Encyclopedia of Sociology*.

Chang, M. Y. (2016). Mobile Banking: The Best Hope for Cyber Security Development. *U. Ill. L. Rev.*, 1191.

Communications Authority of Kenya (2021). Accessed via https://www.ca.go.ke/cyber-threats-on-the-rise-with-increased-reliance-on-icts-in-the-mitigation-of-covid-19 on 25th Aug 2022.

Daniela, B., Simona, M., & Dragos, P. (2010). Electronic banking advantages for financial services delivery. *Annals of Faculty of Economics*, *1*(2), 672-677.

Das, S., & Dhar, P. (2014). Technological Security Aspects for Internet Banking. *Indian Journal of Research*, *3*(6), 110-115.

Granić, A., & Marangunić, N. (2019). Technology acceptance model in educational context: A systematic literature review. *British Journal of Educational Technology*, *50*(5), 2572-2593.

Hagger, M. S. (2019). The reasoned action approach and the theories of reasoned action and planned behavior.

He, W., Tian, X., Shen, J., & Li, Y. (2015). Understanding Mobile Banking Applications' Security risks through Blog Mining and the Workflow Technology.

Huang, S. M., Shen, W. C., Yen, D. C., & Chou, L. Y. (2011). IT governance: Objectives and assurances in internet banking. *Advances in Accounting*, *27*(2), 406-414.

Islam, M. S. (2014). Systematic literature review: Security challenges of mobile banking and payments system. *International Journal of u-and e-Service, Science and Technology*, *7*(6), 107-116.

Jethwani, K., & Surbhi, G. (2015). Cyber Crime: Issues and Challenges. Delhi: International Journal of Emerging Research in Management &Technology.

Kaspersky report (2021). Accessed via https://kenyanwallstreet.com/cyber-attacks-edge-up-59-in-q2-2021 on 25th Aug 2022.

Khalil, K., Usman, A., & Manzoor, S. R. (2020). Effect of Cyber Security Costs on Performance of E-banking in Pakistan. *Journal of Managerial Sciences, 14*.

Khan, H. F. (2017). E-banking: Benefits and issues. *American Research Journal of Business and Management*, *3*(1), 1-7.

Kim, S., Jeong, S. H., & Hwang, Y. (2013). Predictors of pro-environmental behaviors of American and Korean students: The application of the theory of reasoned action and protection motivation theory. *Science Communication*, *35*(2), 168-188.

Kouraogo, Y., Zkik, K., Idrissi, N. E. J. E., & Orhanou, G. (2017). Security model on mobile banking application: attack simulation and countermeasures. *International Journal of Intelligent Enterprise*, *4*(1-2), 155-167.

Nduta, R. W., & Wanjira, J. (2019). E-Banking Strategy and Performance of Commercial Banks in Kenya. *International Journal of Current Aspects*, *3*(V), 147-165.

Njoroge, M. N. & Mugambi, F. (2018). Effect of electronic banking on financial performance in Kenyan commercial banks: Case of Equity bank in its Nairobi Central Business District branches, Kenya. *International Academic Journal of Economics and Finance, 3(2), 197-215*

Rajarajeswari, P., Sreevani, M., & Suryakumari, P. L. (2021, November). Secure Cloud Risk Architecture analysis for Mobile Banking system and its performance analysis based on Machine learning approaches. In *Journal of Physics: Conference Series* (Vol. 2089, No. 1, p. 012007). IOP Publishing.

Sarjiyus, O., Oye, N. D., & Baha, B. Y. (2019). Improved online security framework for e-banking services in Nigeria: A real world perspective. *management*, *6*, 7.

Trafimow, D. (2009). The theory of reasoned action: A case study of falsification in psychology. *Theory & Psychology*, *19*(4), 501-518.

Uddin, M. H., Mollah, S., & Ali, M. H. (2020). Does cyber tech spending matter for bank stability? *International Review of Financial Analysis*, *72*, 101587.

Wani, T. A., & Ali, S. W. (2015). Review & Scope in the Study of Adoption of Smartphones in India. *Journal of General Managment Research*, *3*(2), 101-118.

Webb, P., Pollard, C., & Ridley, G. (2006, January). Attempting to define IT governance: Wisdom or folly? In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)* (Vol. 8, pp. 194a-194a). IEEE.