Global Scientific JOURNALS

GSJ: Volume 8, Issue 7, July 2020, Online: ISSN 2320-9186
www.globalscientificjournal.com

PROPOSED OCTAVE-SMALL BASED SECURITY FRAMEWORK FOR MOBILE BANKING AMONG COMMERCIAL BANKS IN DEMOCRATIC REPUBLIC OF CONGO

Olivier Fumbu Makeusa[1], Dr. Chao Mbogo[2]Kamotho Njenga[2]

1 MSc Scholar, Computer Information Systems, Kenya Methodist University, Kenya

2 Computer Information Systems, Kenya Methodist University, Kenya

*Correspondence email:makeusafumbu@gmail.com

ABSTRACT

Most customers of commercial banks in the Democratic Republic of Congo have been losing vast amounts of money from their accounts to fraudsters and hackers, who are taking advantage of weak security controls. This has necessitated the present study to be conducted for recommending a mobile banking security framework based on Octave-small approach for commercial banks in the Democratic Republic of Congo.The study adopted a descriptive research design and used 549 branches of the eighteen commercial banks in Democratic Republic of Congo, where theKrejcieandMorgan formula was adopted in obtaining a sample size of 227 respondents. The study findings show that asidentifying critical organisational information has a statistically significant positive influence; identifying threats to information systems critical assetshad a statistically significantpositive influenced; there is statistically significant and positive influence of analysing infrastructure vulnerabilities; and risk mitigation has a statistically significant positive influence on mobile banking among commercial bank in Democratic Republic of Congo. The study recommends anoctave-s based mobile banking security framework comprising of five processes; defining sensitive organizational M-Banking information, identify the security requirements of the vital asset, creating key components of vulnerabilities, create a risk profile for each asset, and developing a corporate security policy and mitigation strategy.

Key Words:Commercial Banks, Critical Organizational Information, Infrastructure Vulnerabilities, Mobile Banking Security Framework, Protection Security Strategy and Mitigation Plan, Risks, Threats

Introduction

The dynamically changing global information infrastructure is offering universal connectivitythrough internetas an invaluable business tool for the banking industry (Betelhem, 2017; Uvaneswaran. Kassa& Hamid, 2017).Recent development in electronic commerce (E-commerce) are equally advancing developments in Electronic banking (E-banking) through employment of the state-of-the-art technology from its new unique characteristics; speed, efficiency, diminishing the expenses, and availing benefit of the unique opportunities

(Uvaneswaran *et al.*, 2017).These developments in e-banking services has led to emergence of: Automated Teller Machine (ATM), Point of Sale Terminal (POS), Internet banking (I-Banking) and mobile banking (M-banking). M-banking, being among the latest discoveries, is prominently enabling customers to perform their banking activities anywhere, at any time, and an affordable cost; adding more convenience for accessing banking services as well as bringing new opportunities to both the formally banked and the unbanked (Desisa&Beshah, 2014).
However, M-banking has itsshare of associated risks, with each stakeholder; financial service consumers, financial providers, carriers, and the financial system, having own share of risk and security concerns (Ashraf, 2012). The most vulnerable in this group are the consumers and financial service providers, who are exposed to unique security issues that are introduced by offering internet banking on a mobile device (Bankable Frontier Associates, 2008). It is for this reason that Bankable Frontier Associates (2008) indicates that moving to a prudent and adjusted security strategy requires a proportionate security framework within which to ensure ongoing and active risk management. This demands for Mobile Financial Service Providers (MFSP) to assess their risks and develop strategies to mitigate them on an ongoing basis. The approaches of risk management methods are mainly classified into quantitative and qualitative (Ganthan, Rabiah&Zuraini, 2009). While quantitative risk management methods use numerical results that express the probability of each risk factor and its effects on the objectives of the organisation (Mazareanu, 2007), qualitative risk management assesses the effects of the identified risk factors and then creates priorities used to decide on how to solve the potential risk factors (Panda, 2009). Since the qualitative approach tend to be simpler to implement than quantitative methods because they utilise the security jargon that non-technical people may be familiar with, it is a better choice for use in the banking sector.

The most popular qualitative risk management methods are Hazard and Operability study (HAZOP), Failure Mode and Effects Analysis (FMEA) or Failure Mode and Effects Criticality Analysis (FMECA), and United Kingdom (UK) Government's Risk Analysis and Management Method (CRAMM) (Panda 2009). Most of these qualitative risk techniques pose severe problems in that they either require highly trained technical teams to perform risk assessment and analysis, are labour intensive (Elyse, 2007; Beachboard *et al.*, 2008). However, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method does not require highly technical people or strong financial support to be implemented, rendering it the most appropriate information security risk management method for use in organisations where there are limited experts in information security risk management (Panda, 2009). In light of this, this study on proposing a security framework for mobile banking among commercial banks in Democratic Republic of Congo (DRC) employed OCTAVE, which is designed to leverage the experience and expertise of people within the organisation.

The OCTAVE approach is driven by two of the aspects: operational risk and security practices, which enables an organisation to refine the view of its current security practices (Alberts &Dorofee 2004). OCTAVE approach allows information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information-related assets. All aspects of risk (assets, threats, vulnerabilities, and organisational impact) are factored into decision making, enabling an organisation to match a practice-based protection strategy to its security risks. Certain variations of the OCTAVE approach offer a choice of risk management techniques suitable to an organisation depending on the size and layering of its information systems (Panda, 2009). Sosonkin (2005) argues that OCTAVE-small (OCTAVE-S) allows organisations to tend to benefit from the catalogue of practices, threat profile, and catalogue of vulnerabilities.

Empirical studies have established that loses incurred by customers, who are using M-banking, are mainly due to weak security controls emanating from banks' ineffective security framework. However, most M-banking security frameworks are designed in the context of developed economies, limiting their applicability to developed countries. This has denied developing economies such as the Democratic Republic of Congo' the much-needed information for implementing competitive M-banking security frameworks, knowledge gap. The existence of these gaps thus necessitates a need to rationalize the use of an OCTAVE-S based security framework for mobile baking among commercial banks in the Democratic Republic of Congo.

The objective of this study was to recommend a security framework based on the octave-small approach for mobile banking among commercial banks in the Democratic Republic of Congo. So as to achieve this objective, the study; identified critical organizational information, threats to information systems critical assets, infrastructure vulnerabilities, and risks prompting and protection and mitigation strategies as helpful in designing a security framework for the mobile banking among commercial bank in Democratic Republic of Congo.

Research Methodology

The study used a descriptive research design to identify, analyse and assess the critical factors necessary for the development of a mobile banking security framework for commercial banks in the Democratic Republic of Congo. This design was used to gather data on mobile banking security frameworks. The data was analysed using quantitative analysis to yield descriptive statistics which were used in multiple regression analysis for estimate a study model.
The current study identified the target population as the 549 commercial bank IT managers in the Democratic Republic of Congo (DRC).

The study used the formula $\boldsymbol{s = \chi 2NP\ (1 - P)\ /\ [d^2\ (N - 1) + \chi 2P\ (1 - P)]}$ by Krejcie*and* Morgan (1970) to obtain a sample size of 227 respondents from a target population of 549. In formula;

s = required sample size.

$\chi 2$ = the table value of chi-square for 1 degree of freedom at the desired confidence level (3.841).

N = the population size.

P = the population proportion (assumed to be .50 since this would provide the maximum sample size).

d = the degree of accuracy expressed as a proportion (.05).

Given the sample size = $s = \chi 2NP\ (1 - P)\ /\ [d^2\ (N - 1) + \chi 2P\ (1 - P)]$

Then s = [3.841 x 549 x 0.5 (1 – 0.5)]/ [0.05 x0.05 (270-1) + 3.841 x 0.5(1- 0.5)]

= (3.841 x 549 x 0.5 x 0.5)/ [(0.05 x0.05 x 548) + (3.841 x 0.5 x 0.5)]

= 527.18/ (1.38+ 0.96)

= 527.18/ (2.34)

= 226.23

≈ 227

Therefore, the sample size was 227 respondents from the 549 branches of the eighteen commercial banks in DRC.The study then used proportionate stratified sampling to establish the sample size from each bank and obtained the respondents using simple random sampling.

A structured questionnaire was administered to the 227 respondents, which was designed using 5 points Likert scale (1 - 5), using the drop and pick methods.Before the study embarked on active data collection, it was first tested for validity and reliability using content validityand Cronbach alpha internal reliability test.During data analysis, quantitativeanalysis technique was used to produce the associated descriptive statistics.Analysis of Variance (ANOVA) was used to test the hypotheses, and multiple regression use for predicting the modelthat would explain the dependent variable in terms of the independent variables.The data analysis was done with help of SPSS (Statistical Package for Social Sciences) software version 22.0.

Results and Discussions

The study analysed the dependent variable and the study objectives using the answers obtained using the questionnaire, where the questions were measured using 5point Likert scale (1 – 5). Which were; Strongly Disagree = 1: Disagree= 2: Neutral = 3: Agree = 4: Strongly Agree = 5. The study produced Mean (M) and standard deviation (SD) of the results, which were transformed into continuous data such that ; 1 to 1.8 for Strongly Disagree, above 1.8 to 2.6 for Disagree, above 2.6 to 3.4 for Neutral, above 3.4 to 4.2 for Agree and 4.2 to 5.0 for Strongly Agree.

Critical organisational information

The study assessed theprotection of critical organizational information by the existing mobile banking security framework among commercial banks in DRC to yield results in Table 1.

Table 1: Analysis by critical organizational information

Critical organisation information	M	SD
Key information technology systems are properly protected in our bank	2.43	0.89
The banks critical assets are have never been attacked by any threats	3.07	1.11
Security requirements for critical assets are properly followed in our bank	2.97	1.36
Areas of concern are not subjected to any threat	2.35	1.28
Threats to impact descriptions have never affected the mobile banking	3.78	0.72
Threats to current security practices are always mitigated	3.89	0.45
Averagecritical organisation information	**3.08**	**0.97**

Source: Research data (2019)

These results show that critical organizational information had a moderate influence the development of mobile security framework among commercial banks in DRC(M=3.08, SD= 0.97). The key information technology systems were not properly protected in their bank (M=2.43, SD=0.89)and the areas of concern were subjected to some threats(M= 2.35, SD=1.28). The results show that the banks' critical assets were sometimes attacked by some threats (M= 3.07, SD=1.11). Further, security requirements for critical assets were moderately properly followed in their banks.(M= 2.97, SD=1.36) the threats to impact descriptions had never affected the mobile banking(M=3.78, SD=0.72). However, threats to current security practices were always mitigated(3.89, SD=0.45).

The results on the level of occurrence of the threats in their computer information system (CIS)are shown in Table 2.

Table 2:Level of occurrence of common threats

Level of occurrence of common threats	**M**	**SD**
Decommissioning	3.91	0.72
Lack of awareness	3.65	1.00
User permission fatigue	3.51	1.08
No privacy protection best practice	3.58	0.83
Phishing	4.24	0.86
Spyware	3.44	1.27
Spoofing attacks	4.04	0.64
Diallerware	3.57	0.82
Vulnerabilities leading to malware installation	3.37	1.25
Data leakage	2.03	0.81
Unintentional data disclosure	3.47	0.86
Surveillance	2.72	1.10
Application malfunction	3.09	1.31
Encryption weaknesses	2.76	1.25
Weak app. Distributor authentication mechanism	2.47	1.59
Weak sandboxing	3.22	1.27
Risk of mismanagement of the above threats if not adequately addressed by the organization	3.29	1.26
Averagelevel of occurrence of threats	3.32	1.05

Source: Research data (2019)

As shown in table 2 above the respondents showed there was moderate occurrence of threats on the banks' CIS (M=3.32, SD = 1.05). Based on these results, the respondents were able to classify the threats by their level of occurrence where the levels were low, medium, high and very high. Each of data leakage (M=2.03, SD = 0.81), weak application distributor authentication mechanism (M=2.47, SD=1.59) was shown to have had a low influence. Also, each of; surveillance (M=2.72, SD=1.10), encryption weaknesses (M=2.76, SD=1.25), application malfunction (M=3.09, SD=1.31), weak sandboxing (M=3.22, SD=1.27), risk of mismanagement of the threats if not adequately addressed by the organization (M=3.29, SD=1.26) and vulnerabilities leading to malware installation (M=3.37, SD=1.25) was shown to have had medium level of occurrence. Each of the variables; spyware (M=3.44, SD=1.27), unintentional data disclosure (M=3.47, SD= 1.26), user permission fatigue (M=3.51, SD=1.08), lack of awareness (M=3.65, SD=1.00), no privacy protection best practice (M=3.58, SD=0.83), diallerware (M=3.57, SD=0.82), decommissioning (M=3.83, SD=0.83), congestion (M=3.92, SD=0.79) and spoofing attacks (M=4.04, SD=0.64) was said to have had high level of occurrence. The respondents showed that phishing (M=4.24, SD=0.86) had a very high level of occurrence as shown by the respondents in the table above.

These findings in this section are evidence of the study Moyo (2014) which found that main threats to these critical assets were authorized and unauthorized systems users, malware, system crashes, access paths and incompatibilities in software.In his study, Ashraf (2012) identified eight threats: users, phones, apps and data, and management. Based on this categorization and interviews with banking and IT security professionals. Ashraf (2012) had meanwhile discovered that specific threats occur when dealing with mobile banking safety aspects which include; properly addressing the privacy, credibility and availability of mobile safety resources by safety monitoring and measures. Mobile security tools, the mobile app and private information therefore require protection.

Threats to information systems critical assets

The study established threats to effects of information systems on critical assets as shown in Table 3

Table 3: Effects of threats on information systems critical assets

Effects of threats on information systems critical assets	**M**	**SD**
Current threats and vulnerabilities affect the customers' mobile data in way	3.03	1.09
Our bank has never experienced any disclosure of customers mobile information	3.60	1.30
There has never been any modification customers mobile information in our bank	2.61	1.47
There has never been any occurrence of interruption on customers mobile information	1.32	0.57
Average effects of threats to information critical assets	**2.64**	**1.11**

Source: Research data (2019)

The respondents indicated that the threats had a moderate effect on critical information systems of the banks (M=2.64, SD=1.11) while these threats and vulnerabilities moderately affected the customers' mobile data in anyway (M=3.03, SD=1.09). according to these results, their banks had never experienced any disclosure of customers mobile information (M=3.60, SD=1.30) and there had been moderate modification customers mobile information in our bank (M=2.61, SD=1.47).They showed that there had been high occurrence of interruption on customers mobile information (M=1.32, SD=0.57).

Then the study assessed the exposure to threats on information systems critical assets to yield results in Table 4.

Table 4: Exposure to threats to information systems critical assets

Exposure to threats to information systems critical assets	**M**	**SD**
IT specialist have restricted access in the system.	1.32	0.47
Data transfer between the bank and the company is very secure as only a weak encryption is used.	1.41	0.49
The operating systems e.g. of the accounting system have several patches.	2.45	1.35
The firewall is properly configured; websites are not blocked.	2.90	1.47
All used and active administrative accounts in MS Active Directory.	2.59	1.44
There is appropriate disaster recovery and business continuity documentation.	2.75	1.45
Documents and information were securely stored	2.95	1.22
Confidential information is securely stored	2.75	0.92
Average exposure to threats to information systems critical assets	**2.39**	**1.10**

Source: Research data (2019)

The respondents showed that the exposure to threats on information systems critical assets was low (M=2.39 SD=1.10). They strongly disagreed with the notion that IT specialist have restricted access in the system (M=1.32, SD=0.47) and that data transfer between the bank and the company is very secure as only a weak encryption is used (M=1.41, SD=0.49). The respondents disagreed that the operating systems e.g. of the accounting system have several patches (M=2.45, SD=1.35). They were neutral on all other indicators including; all used and active administrative accounts in MS Active Directory (M=2.59, SD=1.54); confidential information is securely stored (M=2.75, SD=0.92); there is appropriate disaster recovery and business continuity documentation (M=2.75, SD= 1.45); the firewall is properly configured; websites are not blocked (M=2.90, SD=1.75) and documents and information were securely stored (M= 2.95, SD=1.22).While the study respondents indicated that there were no exposures to threats to information systems critical assets (M=2.39 SD=1.10). The study by Moyo (2014) found that risks posed by threats were caused by unavailability of critical information systems assets, compromise of data integrity and confidentiality. This leads to the loss of productivity and damage to organisation’s reputation. In regards to this, the threats lowly influenced information system critical assets. IT specialists did not have restricted access in the system with data transfer between the bank and the company being is not as secure as only the weak encryption used.

Infrastructure vulnerabilities

The study assed the mitigation on infrastructure vulnerabilities and produced results in Table 5

Table 5: Mitigation of infrastructure vulnerabilities

Mitigating infrastructure vulnerabilities	M	SD
Key components for critical assets are protected against vulnerabilities in our bank	2.88	1.00
Technical vulnerabilities on customer mobile data are properly mitigated	3.08	0.78
Current technological vulnerabilities do not affect customer mobile data	3.05	0.91
vulnerabilities for key customer mobile data components are always diverted	3.34	0.97
Our bank provides a very high level of deterrence and (or) defense provided on customer mobile data	2.97	0.91
Average mitigating infrastructure vulnerabilities	3.06	0.92

Source: Research data (2019)

The results showed that the infrastructure vulnerabilities were moderately mitigated (M=3.06, SD=0.92).The key components were moderately protected against vulnerabilities (M=2.88, SD=1.00)while technical vulnerabilities were moderately mitigated(M=3.08, SD=0.78). Current technologies partially affected customer mobile data(M=3.05, SD= 0.91), vulnerabilities for key customer mobile data components were moderately diverted (M=3..34, SD= 0.97)and the banks provided average level of deterrence on customer mobile data(M=2.97, SD= 0.91). Furthermore, the study Taubenberger (2014) proposes that information assets' security requirements are evaluated in the context of the business process model, in order to determine whether security functions are implemented and operating correctly.

Risks Mitigation

The study analyzedmitigation of risks in the current mobile banking security framework for commercial banks in DRC and produced results in Table 6.

Table 6:Risks to CIS

Risks	**M**	**SD**
Risk to organizational customer mobile banking information is always mitigated	3.03	0.75
There are no risks to critical customer mobile banking assets	2.75	0.62
Our banks information always detects risk occurrence on customer mobile banking	2.34	1.26
Average Risks	**2.71**	**0.87**

Source: Research data (2019)

The respondents were neutral on the assertion that risks on mobile banking were mitigated (M=2.71, SD=0.87). The respondents disagreed that their banks information always detect risk occurrence on customer mobile banking (M=2.34, SD=1.26). They were however neutral that Risk to organizational customer mobile banking information is always mitigated (M=3.03, SD=0.75) and that there are no risks to critical customer mobile banking assets (M=2.75, SD=0.62).

Respondents also provided details on the level on which CIS assets were prone to risk to produce results in Table 7.

Table 7: Level of CIS assets proneness to risks

Level of CIS assets proneness to risks	M	SD
Computers especially those used for online banking.	1.91	0.28
Records program	1.81	0.84
Customers' accounts	1.53	0.64
Customers reports	1.72	1.18
Back-up disks stored the strong room	3.16	1.60
Company records	3.23	1.20
Company information	3.60	1.42
Router and the network equipment	3.30	1.39
Average Level of effect of CIS assets prone to risks	**2.53**	**1.07**

Source: Research data (2019)

The respondents were neutral on the assertion that risks on mobile banking were mitigated (M=2.71, SD=0.87). However, risks to organizational customer mobile banking information were moderately mitigatedmoderatelywhile risks were sometimes observed to critical mobile banking assets(M=2.75, SD=0.62).

On risks, the results show that the IS assets were lowlyprone to risk (M=2.53, SD=1.07). Indicators such as customer's accounts (M=1.53, SD=0.64), records program (M=1.81, SD=0.84) and customers reports (M=1.72 SD=1.18) were observed not to have been influenced according to the respondents. Computers especially those used for online banking (M=1.91, SD=0.28) were said to have been lowly influenced. Back-up disks stored the strong room (M=3.16, SD=1.60) and company records (3.23, SD=1.20), and router and the network equipment (M=3.30, SD=1.39) were moderately influenced. However, company information (M=3.60, SD=1.42) highly influenced according to the respondents. The findings confirm Janulevicius's (2016) study which concluded that the automation of virtualization solution risk analysis provides sufficient data for adjustment and implementation of security controls to maintain optimum security level.

Analysis of Variance (ANOVA) was used to test the goodness of fitness of the model and these results are captured in Table 8

Table 8: ANOVA for Security Framework for commercial banks in DRC

ANOVA[a]

	Sum of Squares	df	Mean Square	F	Sig.
Regression	30.493	4	7.623	17.65	.000[b]
Residual	78.606	182	0.432		
Total	109.099	186			

a. Dependent Variable: Mobile banking security framework among commercial banks in Democratic of Congo

b. Predictors: (Constant), Risks, Threats to information systems critical assets, Infrastructure Vulnerabilities, Critical organisational information

Source: Research data (2019)

The study tested the fitness of the model at 5% level of significance to find that the probability value (p-value) was 0.000 which was less than 0.05. This implies that at α=0.05, there exists enough evidence to conclude that at least one of the IVs; identifying critical organisational information, identifying threats to information systems critical assets, analysing infrastructure vulnerabilities, and protection security strategy and mitigation plan wasuseful in estimating the mobile banking Security Framework for commercial banks in DRC and hence the model is relatively suitable in explaining the variance of levels of security framework for commercial banks in DRC as explained by the variance in these factors.

The regression results to estimate the study model are shown in Table 10.

Table 9: Regression Results of Dependent Variable against Predictor Variables

Coefficients[a]

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	0.592	0.336		1.763	0.080
Identifying critical organisational information	0.151	0.062	0.163	2.428	0.016
Identifying threats to information systems critical assets	0.149	0.048	0.195	3.087	0.002
Analysing infrastructure vulnerabilities	0.152	0.074	0.137	2.047	0.042
Protection security strategy and mitigation plan	0.304	0.051	0.381	5.936	0.000

a. Dependent Variable: Mobile banking security framework among commercial banks in Democratic of Congo

Source: Research data (2019)

These results show that each explanatory variables;Identifying critical organisational information (p-value = 0.016), identifying threats to information systems critical assets (p-value = 0.002), analysing infrastructure vulnerabilities (p-value = 0.042), and protection security strategy and mitigation plan (p-value = 0.000), had p-values of less than the 0.05. So,they were goodestimators of security framework for commercial banks in DRC. The coefficient for identifying critical organisational information (β_1= 0.151), identifying threats to information systems critical assets (β_2= 0.149), analysing infrastructure vulnerabilities (β_3= 0.152), and protection security strategy and mitigation plan (β_4=-0.304) were used to estimated model fitted as;

$Y = 0.592 + 0.151X_1 + 0.149X_2 + 0.152X_3 + 0.304X_4$……………………. (i)

The fitted regression equation is in the form of Security Framework for commercial banks in DRC = 0.592 + 0.151 (identifying critical organisational information) + 0.149 (identifying threats to information systems critical assets) + 0.152 (analysing infrastructure vulnerabilities) + 0.304(protection security strategy and mitigation plan).

Table 10: Model Summary for Security Framework for commercial banks in DRCs

Model Summary

R	R Square	Adjusted R Square	Std. Error of the Estimate
.529[a]	0.2795	0.2637	.65719

a. Predictors: (Constant), protection security strategy and mitigation plan, identifying threats to information systems critical assets, analysing infrastructure vulnerabilities, identifying critical organisational information

Source: Research data (2019)

Table 20 shows the coefficient of determination was .2795, an indication that 27.95% of variation in Security Framework for commercial banks in DRCs is explained by change in; identifying critical organisational information, identifying threats to information systems critical assets, analysing infrastructure vulnerabilities, and protection security strategy and mitigation plan. Therefore, all the variable; identifying critical organisational information, identifying threats to information systems critical assets, analysing infrastructure vulnerabilities, and protection security strategy and mitigation plan are strong determinants of Security Framework for commercial banks in DRC**.**

Conclusions

The study concludes that identifyingcritical organisational information has a statistically significant and positiveinfluence on the development of mobile banking security framework among commercial banks in DRC. The core consideration in developing the framework are; properly addressing information technology systems, addressing attacks on banks critical assets, ensuring properly following security requirements for critical assets, and mitigating threats to security practices

The study concludes that the identification of threats to critical M-banking assets has statistically significant and positively influences design of mobile banking security framework for commercial banks in DRC. This is characterized by restrictions of IT specialists access on the system with data transfer between the banks, strength of encryption used, level of operating patches, used and active administrative accounts in MS Active Directory; security storage of confidential information; presence of appropriate disaster recovery and business continuity documentation; configuration of firewall; staff awareness of IS threats and secure storage of information.

The study concludes that there is statistically significant and positiveinfluence of analysing infrastructure vulnerabilities moderately on the design of the mobile banking security framework. The key components for consideration are for protection against these vulnerabilities, addressing technical vulnerabilities, mitigating current technologies, protecting against vulnerabilities on key customer mobile data components, and providing high level of deterrence on customer mobile data.

The study concludes that risk mitigations (protection security strategy and mitigation plan)has a statistically significant and positive influence in the design of mobile banking security framework. The core consideration in risk mitigation are; detecting risk occurrence on customer mobile banking, mitigation of risks to organizational customer mobile banking information, customer accounts, records program, customer reports, protection of computers especially those used for online banking, back-up disks stored the strong room and company records. There is an important need to protect router and the network equipment and company information.

Recommendations

Proposed Framework

The study proposes for a proportionate regulatory framework which ensures that commercial banks in Democratic Republic of Congo maintains active risk management in its mobile banking. Thus, the study recommends for development of a comprehensive risk framework for banks offering M-Banking services. It also recommends for mFSPs to create a flexible, proportionate framework within which an on-going, active supervision of mFSPswould take place. This would ensure adequate attention in identifying, monitoring and controlling the mobile channel risks while providing adequate room for risk appropriate innovations that might be excluded if entrenched, inflexible technology standards exist.

OCTAVE-Sshould be used during the mapping of data resources with the help of information producers and users of M-banking. organizations are engaged in a public dialog to explore genres in which data is transmitted through supporting resources. In addition, the identified information assets for further risk assessment are incorporated into OCTAVE-S. Accordingly, the suggestsimplementation of anoctave-s based framework with five processes, where;

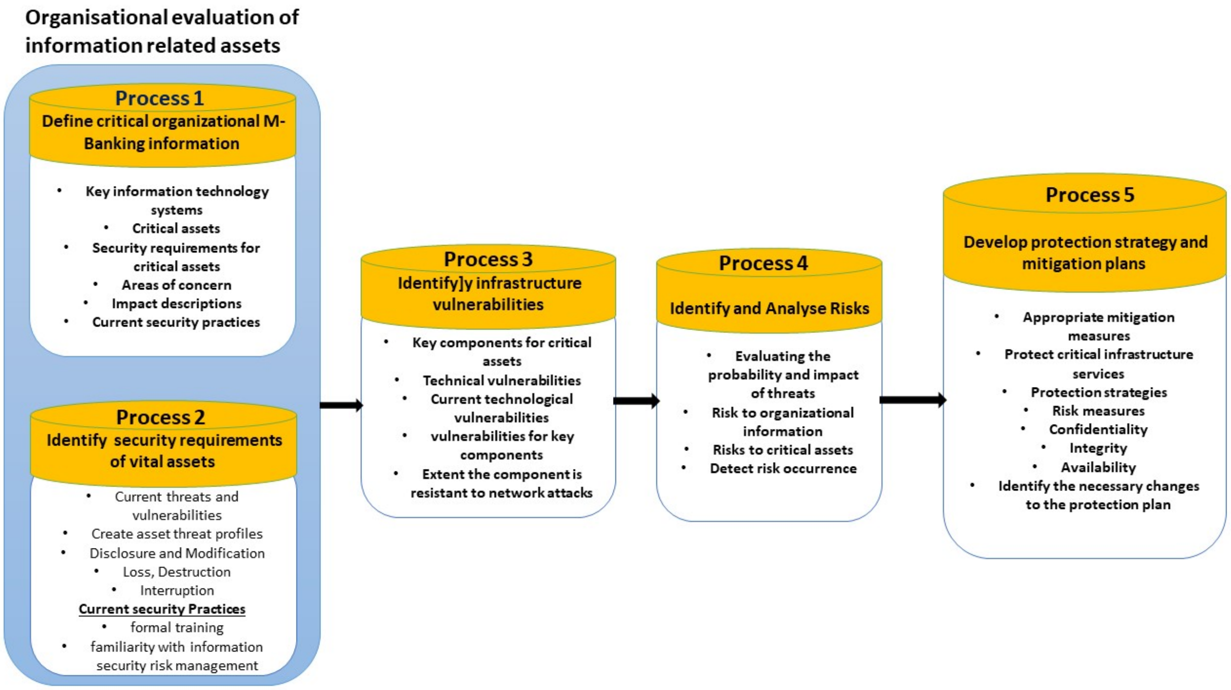
Processone will include defining sensitive organizational information in order to set up a special group for M-Banking offering banks to recognize essential M-Banking information resources and to develop a collection of impact requirements and current security practices for banks. The information obtained is significant for the creation of resource-based risk profiles.

Process two is to recognize the risks to vital information system resources by assessing the facets of the bank in which users of the data system contribute their views on what is relevant and what is being done to protect those assets by the bank. The project team would then identify the security requirements of the vital asset and then create a risk profile for each asset. The risk profile should be established; the information previously obtained from the various users of critical information assets should be grouped; the critical assets identified and the threat profile established for each critical asset. The group should also assess whether the consequences of the identified threats lead to; disclosure or representation of sensitive information; alteration of valuable or sensitive data; destruction or degradation of important information; interruption of access to significant information, technology, applications or services.

Process three involves finding vulnerabilities in infrastructure Key components of vulnerabilities are being checked (technological vulnerabilities) that could contribute to unauthorized action on sensitive property. This is a high-level survey to refine the threat profiles of infrastructure and technology practices. Physical reviews of computer hardware and components would be conducted to identify vulnerabilities that could be abused by threats.

Process four and five includes a risk analysis and implementation of security management measures and mitigation plans. The group must define, assess and then take decisions on all risks to the core resources of the company. The group should now develop a corporate security policy and mitigation strategy to address the threat to critical resources based on information collected from research. The impact and probability of all identified risks will be qualitatively assessed in the risk analysis.

The proposed framework model captured hereunder should lead to the development of an organizational security policy and risk mitigation plan based on findings from process one to five


Organisational evaluation of information related assets
Process 1
Define critical organizational M-Banking information
• Key information technology systems
• Critical assets
• Security requirements for critical assets
• Areas of concern
• Impact descriptions
• Current security practices
Process 2
Identify security requirements of vital assets
• Current threats and vulnerabilities
• Create asset threat profiles
• Disclosure and Modification
• Loss, Destruction
• Interruption
Current security Practices
• formal training
• familiarity with information security risk management
Process 3
Identify]y infrastructure vulnerabilities
• Key components for critical assets
• Technical vulnerabilities
• Current technological vulnerabilities
• vulnerabilities for key components
• Extent the component is resistant to network attacks
Process 4
Identify and Analyse Risks
• Evaluating the probability and impact of threats
• Risk to organizational information
• Risks to critical assets
• Detect risk occurrence
Process 5
Develop protection strategy and mitigation plans
• Appropriate mitigation measures
• Protect critical infrastructure services
• Protection strategies
• Risk measures
• Confidentiality
• Integrity
• Availability
• Identify the necessary changes to the protection plan

Octave-s based Proposed framework model

Recommendations on Research Findings

The study made recommendations based on study findings as well as for future research, which are contained in this section. The study found that 27.95% of change in Mobile banking security framework among commercial banksin DRC is explained by; identifying critical organisational information has positive significant, identifying threats to information systems critical, analysing infrastructure vulnerabilities, and protection security strategy and mitigation. This means there are other factors accounting for the remaining 71.05%. The study therefore, recommends that other studies should be conducted to establish what contributes to the 71.05% variation in Mobile banking security framework among commercial banks in DRC.

Further studies should be done to assess the viability of the framework in other banking industry.

References

Alberts, C. J. &Dorofee, A. (2002). *Managing information security risks: The OCTAVE SM approach.* Boston: Addison-Wesley Anderson

Alberts, C. J. &Dorofee, A. (2003). *Managing information security risks: the OCTAVE approach*, Pearson Education, Inc. Boston

Alberts, C., Dorofee, A., Stevens, J. & Woody, C. (2003*). Introduction to the OCTAVE® Approach*. Pittsburgh, PA: Carnegie Mellon University

Ashraf, I. (2012), *Mobile Banking Security. A security model* (Doctoral Thesis, Vrije Universiteit, Amsterdam, The Hague, The Netherlands).

Audu, J. (2018). *Technology adoption in Democratic Republic of Congo (DRC): An Empirical study investigating factors that influence online shopping adoption* (Master's Thesis, University of Ottawa, Ottawa, Ontario, Canada)

Bankable Frontier Associates. (2008). *Managing the risk of mobile banking technologies*.Bankable Frontier Associates LLC.Retrieved fromwww.bankablefrontier.com.

Betelhem B. G-H. (2017). *Conceptual security framework for mobile banking key authentication and message exchange protocols: Case of Ethiopian Banks* (Master Thesis, St. Mary's University, Addis Ababa, Ethiopia).

BSI (2005) *ISO/IEC 27001:2005 Information technology – security techniques –information security management systems – requirements.* British Standard Institute.

BSI (2008) *ISO/EIC 27005:2008 Information technology — Security techniques — Information security risk management*. British Standard Institute.

Campbell, P, L. & Stamp, J. E. (2004). *A Classification Scheme for Risk Assessment Methods?*, Sandia National Laboratories.Retrievedfrom http://energy.sandia.gov/wp/wp-content/gallery/uploads/sand_2004_4233.pdf.

Douramanis, M. (2014). *Risk assessment for the cyber threats to networked critical infrastructure* (Master's Thesis, Leiden University, Leiden, The Netherlands).

ITGI (2007) *COBIT 4.1*. Rolling Meadows, IL: IT Governance Institute.

GSMA Intelligence. (2016). *The Mobile Economy Africa*. *GSM Association*. Retrieved from www.gsmaintelligence.com

Janulevicius, J. (2016). *Method of information security risk analysis for virtualized systems* (Doctoral dissertation, Vilnius Gediminas Technical University)

Kaur, R. (2014). Control Issues and Mobile Devices.

Keung, Y. A. U. H. (2014).Basic principle of information security.*Advances in Robotics & Automation*, *3*(2), 9695. Retrieved from http://doi.org/10.4172/2168-9695.1000e118.

Kothari, C. R. (2012). *Research methodology: methods and techniques.* New Delhi: New Age International.

Moyo, M. (2014). *Information security risk management in small-scale organisations: A case study of secondary schools? computerised information systems* (Master dissertation, University of South Africa, cape Town, Republic of South Africa).

Ochuko, R. E. (2012). *E-banking operational risk assessment A Soft Computing Approach in the Context of the Nigerian Banking Industry* (Doctoral Thesis, University of Bradford)

Padyab, A. M. (2014), *Towards more structured information asset identification approach for risk assessment methods using genre based Method* (Master's Thesis, Luleå University of Technology).

Rovito, S. M. (2016). *An Integrated Framework for the Vulnerability Assessment of Complex Supply Chain Systems* (Master's Thesis, Massachusetts institute of technology)

Shaaban, H. K. (2014). *Enhancing the governance of information security in developing countries: The case of Zanzibar* (Doctoral Thesis, University of Bedfordshire).

Sosonkin, M. (2005). *OCTAVE: Operationally Critical Threat, Asset and Vulnerability Evaluation*.Retrieved from http://isis.poly.edu/courses/cs996-management-s2005/Lectures/octave.pdf.

Storms, A. (2003). *Using vulnerability assessment tools to develop an OCTAVE risk profile*. Retrieved from http://www.sans.org/reading_room.

Taubenberger, S. (2014). *Vulnerability Identification Errors in Security Risk Assessments* (Doctoral thesis, The Open University).

Woody, C., Coleman, J., Fancher, M., Myers, C. & Young, L. (2006). *Applying OCTAVE: Practitioners Report*. Retrievedfrom http://www.sei.cmu.edu/publications/pubweb.html/06tn010.pdf.