Data Security Preparedness Levels And Online Banking Services: A Case Study Of Information Technology Department Of Access Bank, Kigali, Rwanda

Dieudonné Muhire, Raymond Wafula Ongus

Mount Kenya University, Kigali campus, Rwanda, School of Pure and applied science, Department of Information Technology
Email: dmuhire1@gmail.com, raymondongus@gmail.com

ABSTRACT: Data security has been the main approach to deal with loss of data. The motivation of this study was inspired by the continuing concern of ineffective data/information security in companies leading to considerable monetary losses. The aim of this study was to examine the main causes of data insecurity and to establish how data security preparedness levels at Access Bank, Kigali, Rwanda affect online banking services. This study used questionnaires and interviews for data collection. All fifty nine IT employees and their managers at Access Bank represented the total number of population. Therefore the total population of fifty nine (59) was the sample size. As this was a small population size, a purposive sampling technique was used as a sampling method. After collecting data, the interpretation and the summary of quantitative data was done using statistics such as graphs, frequency tables, weighted means, standard deviations, and percentages to enable describe the relationships established. This was achieved by the use of Statistical Package for the Social Sciences Version 17.0 (SPSS V.17.0) software as the tool of analysis. Findings revealed that internal based attacks are the first major cause of data insecurity in the company as indicated by 50.90% of respondents. The multiple regression found that r the coefficient of correlation was 0.793. This meant that there was strong positive multiple correlation between data security preparedness levels and online banking services at Access Bank, Kigali Rwanda. Moreover the coefficient of determination r^2 =0.628 indicated that 62.8% of the total variation in online banking services depended on stochastic model developed whereas the remaining 37.2% was attributed to factors beyond the control of the study. Since the correlation was strong, this relationship was found to be significant. Recommendations were to give regular assistance to customers to avoid identity theft, to provide training to every employee of the Bank and to introduce additional security measures stated in this study to deal with internal incidents.

Keyword: Information security, Information Communication Technology, data security, online banking services

INTRODUCTION

Previous studies done, have found that security mechanisms for protecting computers systems are widely available, unfortunately despite the protective impact of these mechanisms the problems of data theft, data insecurity and data loss are still rising. Public and private companies all over the world face variety of information threats. Securing their information has become a crucial function within the information systems. Moreover in developed countries, high education researchers have discovered technical issues, non-technical issues of information security as well as their solutions (Salahuddin, 2011). In Africa when it comes to computer security issues, four out of the top ten countries in the world with high level of data insecurity and cybercrime incidence, come from sub-Sahara in Africa (Nigeria, Cameroon, Ghana and South Africa). In terms of solutions to data security issues in Africa, security mechanisms such as: cyber security awareness, capacity and skills improvement, legislative and policy aspects, national computer security incident response teams and more researches on cyber security have been suggested (Kritzinger, 2012). However when it comes to Rwanda, there is a scarcity of studies conducted on data security systems as well as their security issues. Without an effective program for assistance in data security, security incidents will continue resulting in monetary loss. The research problem therefore was an assessment of the effect of data security preparedness levels on online banking services by considering the IT department at Access Bank in Kigali, Rwanda as a case study.

Objectives of the Study

The main objective of this study was to establish how data security preparedness levels at Access Bank, Kigali, Rwanda affect online banking services. The specific objectives of this study were: 1) To assess the root causes of data insecurity at Access Bank, Kigali, Rwanda. 2) To assess the effectiveness of data security measures currently used to implement data security at Access Bank, Kigali, Rwanda. 3) To determine the additional measures to be put in place to improve data security at Access Bank, Kigali, Rwanda. 3) To determine how data security preparedness levels at Access Bank, Kigali, Rwanda affect online banking services.

Data Security Models

Data security models include State Machine Model, Bell-LaPadula Model, Biba Model**,** Clark-Wilson Model, Graham-Denning Model, Brewer Nash Model (McLean, 1995). This study was depended heavily on the Bell-LaPadula model because it was developed to address the concerns of the security of systems and leakage of classified information.

Concepts/Theories of Information Security

All the concepts**,** principles and mechanisms of information security are based on these three fundamental theories of confidentiality, integrity, and availability of information also known as the C-I-A triad or information security triad. Security is traditionally concerned with the information properties of confidentiality, integrity and availability. These properties emphasize on services such as user Identification, authentication, authorisation, accountability and reliability (Stalling, 2011). Main mechanisms of insuring confidentiality of information or data are encryption, Access

Control Lists (ACLs) and Firewalls. Examples of threats to confidentiality are malware, intruders, social engineering, insecure networks, and inadequate administered security systems (Williams, 2007). Integrity security mechanisms may be classified into two types: preventive mechanisms, such as access controls prevent unauthorized modification or change of information, and detective mechanisms, which detect unauthorized modifications or change when preventive mechanisms have failed. If an infringement of integrity is discovered, then the mechanism may report this infringement, and some software or human involvement is required to recover from the infringement. Alternatively, there are mechanisms used to restore at a given point or to recover from the loss and from the violation of integrity of data. The use of backup recovery mechanisms is typically the more outstanding alternative. Backups of data, business continuity and disaster recovery plans (which consist of at least regular backups) are also planned to mitigate losses during natural disasters and human errors therefore ensuring the availability of information (Stallings, 2011).

Research Gap identification

In his study Younus (2009) discovered how to deal with confidentiality of data by using password, biometric systems and token based authentication; Tarushi (2014) focused on providing powerful security mechanisms such as email analysis and data mining for fraud detection and tracing the behavior of an employee; Stewart (2005) described data security as part of the market improvement tactic in e-commerce. Therefore previous studies covered data security as well as their mechanisms but they left out how data security preparedness levels affect online banking services and the assessment of main causes of insecurity for example malicious software, software and hardware failures etc... This was the knowledge gap that the study intended to fill particularly in the case of Rwanda, where published materials in this area of interest are few.

Conceptual Framework

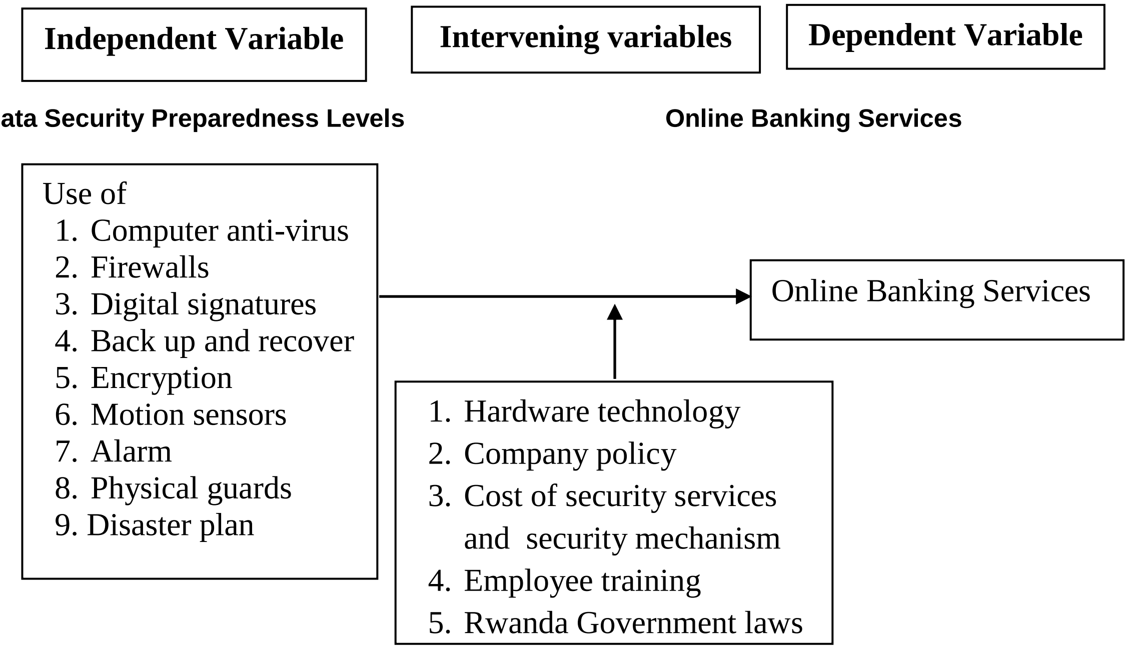

Figure 2.5: *Conceptual Framework*
Source: *(Preliminary interpretation)*

RESEARCH METHODOLOGY

Research Design

This study was based on a descriptive case study research design. This research design was chosen because it was felt to be most suitable to clarify a set of security measures, why they were taken, how they were implemented and with what result in the context of the chosen organization. A case study allows a lot of details to be collected that would not normally be easily obtained by other research design. In this study, the case study discovered how the data security is prepared in financial institutions, what existing causes of insecurity they faced (Salahuddin, 2010).

Target Population and Sample Design

The target population is the group or individuals to whom the survey applies or from which samples are obtained (Kitchenham, 2003). The target population for this study is fifty nine (59) staff of Access Bank, Kigali. This number covered four managers (4) and fifty five (55) IT department staff of Access Bank Kigali Rwanda and it was the number of employees responsible for data security preparedness in the company. Additionally the sampling design of the total population was a census.

Data Collection Procedure

Firstly the fifty five well-structured questionnaires were distributed to the IT department employees who are responsible of data security preparedness, and secondary an interview schedules were conducted targeting the four managers. They were selected because they carry out the daily operations and they are more familiar with the situation of the information security. Thus, their responses were constructive and reliable for this study.

Reliability and Validity

Reliability of the study ensures errors in the study are minimized. Reliability requires the process of research to be consistent allowing any later researcher to follow the exact same procedures and get the same result (Salahuddin, 2011). Firstly to ensure that the content of the questionnaires were reliable, first professionals who have knowledge in the area of study were consulted. Their evaluations were included in order to have reliable instruments. Secondly a pilot study was conducted in order to test the questionnaire before collecting the real data. In order to test the internal validity of the different constructs a Cronbach's alpha test was performed on the questionnaire.

Table 1: *Validity Statistics for Six Respondents for Pilot Test*

	Cronbach's Alpha	N of Items
Effectiveness of data security measures	0.714	5
Root causes of data insecurity	0.648	10
Additional measures to be put in place	0.632	4
How data security preparedness levels affect online banking services	0.709	17

Source: *Preliminary data*

From Table 3.1, the root causes of data insecurity Section one of the questionnaire respondents identify 0.648 value of Cronbach's Alpha; effectiveness of data security measures Section two of the questionnaire, respondents identify Cronbach's Alpha of 0.714; how data security preparedness levels affect online banking services Section three of the questionnaire, respondents identify Cronbach's Alpha of 0.709; Additional measures to be put in place Section four of the questionnaire respondents identify 0.632 value of Cronbach's Alpha. As a result the Cronbach's Alpha of all sections is acceptable. It can be deduced that all sections are valid and reliable because the Cronbach's Alpha is greater than 0.5. However section one is more valid and reliable than section two and three. Based on the comments received from pre-test, modifications were made to the questionnaire for improving their simplicity and clarity before using it in the actual questionnaire. The data collected, comments and suggestions were analysed and gaps between the preliminary questionnaire and the required data were identified.

Data Analysis Procedure

Data analysis is the process of examining, categorizing, transforming and modelling data with the purpose of determining useful information, suggesting conclusions, and supporting decision making based on the processed data. After collecting data, the explanation of all the processing operations was followed including editing, coding, classification and tabulation as listed. Data was summarized using descriptive statistics such as graphs, tables, frequency tables, weighted averages, standard deviations and percentages to enable to describe the relationships established. This was achieved by the use of Statistical Package for the Social Sciences version 17.0 (SPSS V. 17.0). The interview guide was analysed using content analysis. Furthermore to analyze the relationship between one dependent variable and several independent variables, multiple regression analysis was applied. Therefore multiple regression analysis was a suitable way to check the relationship between the independent variable and the dependent variable in this study.The stochastic model developed was as follows:

$$Y=b0+b1X1+b2X2+ \dots\dots\dots + bk\ Xk+ \varepsilon$$

Where Xk represents Independent variable, bk represents coefficient and ε represents unknown factor, and Y represents Dependent variable.

RESEARCH FINDINGS AND DISCUSSION

Presentation of Findings

Questionnaires were distributed to IT department employees. During questionnaire examination process, data were obtained on organizational activities that support the preparation of information security. Data were also obtained based on main causes of insecurity. Furthermore the interview was conducted with managers. It was used to understand further current information security measures used to implement data security and the main causes of data insecurity in Access Bank, Kigali.

Root Causes of Data Insecurity at Access Bank

To investigate the root causes which could contribute to data insecurity at Access Bank, the number of intrusions the company has experienced was first considered. Through this study, fifty five respondents of all branches of Access Bank revealed that the company experienced between one and five intrusion in the last two years.

Table 2: *Major Causes of Security Incidents in the company*

		Ranking and Frequency (%)					
Major Causes of Insecurity	N	1st cause 1	2nd cause 2	3rd cause 3	4th cause 4	5th cause 5	6th cause 6
Virus and malicious software	55	7 (12.70%)	32 (58.20%)	11 (20.0%)	5 (9.10%)	0 (0%)	0 (0%)
System or software failure	55	0 (0%)	2 (3.60%)	7 (12.70%)	3 (5.50%)	26 (47.30%)	17 (30.90%)
Internal based attacks	55	28 (50.90%)	12 21.80%	2 (3.60%)	2 (3.60%)	3 (5.50%)	8 (14.50%)
User's errors	55	0 (0%)	6 (10.90%)	6 (10.90%)	42 (76.40%)	1 (1.80%)	0 (0%)
System Administrator's errors or non compliance	55	17 (30.90%	6 (10.90%)	29 (52.70%)	3 (5.50%)	0 (0%)	0 (0%)
Hardware failure	55	0 (0%)	0 (0%)	0 (0%)	0 0%	26 (47.30%)	29 (52.70%)

Source: *Field data*

Table 2 shows that the first main cause of insecurity was internal based attacks. 28 respondents (50.90 %) considered internal based attacks as the 1stmajor cause of data insecurity in the company. This was followed by viruses and malicious softwares as the second major cause of insecurity. Since 32 (58.20%) respondents out of 55 thought that viruses and malicious software are the 2nd cause of data insecurity at the company. The study also revealed that 29 respondents (52.70 %) out of 55 thought that system administrator's errors or non compliance was the 3rd main cause of data insecurity at the company.

Table 3: *Obstacles and concerns in carrying out better security compliance*

		Ranking and Frequency (%)			
Obstacles of security compliance	**N**	**1st place 1**	**2nd place 2**	**3rd place 3**	**4th place 4**
Lack of awareness and training program	55	39 (70.90%)	11 (20.00%)	5 (9.10%)	0 (0%)
Lack of adequate technology	55	7 (12.70%)	10 (18.20%)	29 (52.70%)	9 (16.40%)
Clear direction in security procedures and roles	55	6 (10.90%)	5 (9.10%)	0 (0%)	44 (80.00%)
Lack of motivation Programs	55	9 (16.40%)	28 (50.90%)	16 (29.10%)	2 (3.60%)

Source: *Field data*

These obstacles were analysed since they may lead to data insecurity in financial organizations. Table 3 shows that, out of 55, 39 (70.90%) respondents argued that a lack of awareness and training program was the 1st major obstacle in implementing a better data security at the company whereas 28 respondents (50.90 %) out of 55 thought that a lack of motivation programs wasthe 2nd obstacle in carrying out security system at the company. Furthermore out of 55, 29 (52.70%) respondents indicated that a lack of adequate technology wasthe 3rd obstacle, while 44 (80.00%) thought that a clear direction in security procedures and roles was the 4th obstacle in carrying out data security. Managers through interview indicated that Access Bank offer regular trainings to their employees, but human resources and other departments do not take part into these regular information security trainings. Only some employees follow special training once in year in Nigeria but not every employee is trained. This indicated the reason why respondents through questionnaire acknowledged a lack of awareness and training program as the 1st major obstacle in implementing a better data security To support the motivation program as the 2nd obstacle, managers through interview highlight that when it comes to motivation the Bank only encourages employees by providing assistance, make them work together, make policy and enforce the related rules and procedures.

Table 4: *Number of occasions, the following security strategies have been carried out every five months*

Data Security strategies	N	Very Often 5	Often 4	Sometimes 3	Rarely 2	Never 1	Weighted Mean	Std.
provide clarifications to customers on security	55	0 (0%)	9 (16.40%)	21 (38.20%)	25 (45.40%)	0 (0%)	2.71	0.737
conduct security violation test	55	17 (30.9%)	27 (49.10%)	11 (20.00%)	0 (0%)	0 (0%)	4.11	0.712
conduct data security audit	55	11 (20.0%)	28 (50.90%	16 (29.10%)	0 (0%)	0 (0%)	3.91	0.701
update security software	55	8 (14.50%)	42 (76.40%	5 (9.10%)	0 (0%)	0 (0%)	4.05	0.488

(SD<0.5 or close to zero -Respondents responses crowded around the weighted mean),
(SD >0.5 or high -Respondents responses dispersed on the responses)
Source: *Field data*

Table 3 provides a summary of number of occasions data security strategies have been carried out at Access Bank every five months. It involves calculation of

weighted means for 5 point Likert scale where the weights are as follows: 5= very

often; 4=often; 3=sometimes; 2= rarely; 1= never.

Weighted

Mean=$\frac{\sum(\text{weights}*\text{observeredfrequencies})}{\sum \text{observedfrequencies}}$

i. Provide clarifications to customers on security

The view of respondents regarding the number of times the company has provided customers with clarifications on data security fell between sometimes and rarely, with a weighted mean of 2.71. However the standard deviation of 0.737 indicated that respondents are dispersed on their responses. Table 4 shows that from a total number of 55, 25 respondents noted that rarely the company provide customers with clarifications on data security whereas 21 respondents pointed that sometimes the company provide customers with clarifications on the security. The majority's view was supported by the managers who indicated that the Bank does not provide clarifications on data security because, they felt regular assistance or clarifications are not necessary to customers and may be costly.

ii. Conduct security violation test

The opinion of the majority of respondents regarding the number of times the company has conducted security violation test, falls between very often and often, with a weighted mean of 4.11. However the standard deviation of 0.712 indicated that respondents are dispersed on their responses. Table 3 illustrates that, out of 55 respondents 27 revealed that the company often conduct a security violation test in order to find the weakness of the system's security; whereas 17 respondents noted that very often the company conduct a security violation test.

iii. Conduct data security audit

The view of the majority of respondents lies between often and sometimes, with a weighted mean of 3.91. However the standard deviation of 0.701 indicated that respondents are dispersed on their responses.This has been highlighted by the fact that most of respondents 28 argued that the company often conduct a data security audit in order to assess and examine the system's security compliance, whereas 16 respondents pointed that sometimes the company conduct a data security audit (Table 4).

iv. Update security software

The view of the best part of respondents falls between very often and often, with a weighted mean of 4.05. The standard deviation of 0.488 indicated that respondents' responses are crowded around the weighted mean. Table 3 shows that out of 55 respondents, 42 indicated that the company often update information security software to limit incidents from viruses while 8highlight that very often the company update information security software.

Effectiveness of Data Security Measures Currently Used

To ensure the effectiveness, managers indicated that the use information security standard is involved. Standards define roles and responsibilities to protect and control access to data and help to identify security policies. Their basic principle is that all stored or kept data should be owned so that it is clear whose task is to protect and control access to that data. Table 5 provides a summary of how effective data security measures are, when implementing data security.

***Table 5:** Data Security Measures*

Data Security Measures	N	Strongly Agree 5	Agree 4	Neutral 3	Disagree 2	Strongly Disagree 1	Weighted Mean	Std.
End users or Employee involvement in data security implementation	55	15 (27.30%)	19 (34.50%)	21 (38.20%)	0 (0%)	0 (0%)	3.89	0.809
Implementation of a documented policy	55	38 (69.10%)	17 (30.90%)	0 (0%)	0 (0%)	0 (0%)	4.69	0.466
Implementation of a data loss prevention policy	55	17 (30.90%)	24 (43.60%)	14 (25.50%)	0 (0%)	0 (0%)	4.05	0.756
procedures to discipline employees	55	27 (49.10%)	20 (36.40%)	8 (14.50%)	0 (0%)	0 (0%)	4.35	0.726
Train employee regularly	55	33 (60.00%)	21 (38.20%)	1 (1.80%)	0 (0%)	(0%)	4.58	0.534

(SD<0.5 or close to zero -Respondents responses crowded around the weighted mean),
(SD >0.5 or high -Respondents responses dispersed on the responses)
***Source:** Field data*

i. End Users or Employee Involvement in Data Security Implementation

In general, findings from Table 5 revealed that the opinion of the majority of respondents, fell between agree and neutral, with a weighted mean of 3.91. However the standard deviation of 0.809 indicated that respondents are dispersed on their responses. Out of 55 respondents, 21 were neutral on the effectiveness of involving users in data security implementation. However 19 respondents agreed on the effectiveness of involving users or employees in data security implementation. The majority's view was backed by managers who argued that they are not sure if involving users, increase data security since only IT employees and managers are involved in its implementation.

ii. A Documented Policy

From Table 5, it can be observed that 38 respondents out of 55, strongly agreed on the effectiveness of documented policy for improving data security system whereas 17 respondents agreed on its effectiveness when protecting data. This washighlightedby weighted average of 4.69 where the opinions of the best part of respondents fell between strongly agree and agree. The standard deviation of 0.466 indicated that respondents' responses are crowded around the weighted mean. In addition managers said that a documented policy has been put in place in order to secure efficiently data by avoiding unintentional or intentional disclosures of sensitive business information caused by employees.

iii. Implementation of a Data Loss Prevention Policy (DLP)

One of DLP policy is a messaging system that insures that employees do not send sensitive data outside the network. It can be used to filter email messages and attachments. It can be shown in Table 5 that 24 respondents out of 55, agreed that the company has been protected by the implementation of a data loss prevention policy while 17 respondents strongly agreed. As a result the DLP has been effective. This wasillustrated by the view of respondents regarding the number of times the company has conducted security violation test, which lied betweenstrongly agreeand agree, with a weighted mean of 4.05. However the standard deviation of 0.756 indicated that respondents are dispersed on their responses.

iv. Identify procedures to discipline employees

Table 5 shows that, 27 respondents out of 55 strongly agreed on the effectiveness of the procedures put in place to discipline employees who violate the security policy and regulations of the company whereas 20 respondents agreed. However the standard deviation of 0.726 indicated that respondents are dispersed on their responses. Since the opinion of respondents regarding the effectiveness of these procedures, fell between strongly agree and agree, with a weighted mean of 4.35, these procedures have been effective. This opinion is backed by managers who indicated that these procedures normally were effective. The Bank implemented these measures by showing employees unwanted behaviour and explained them the consequences. Furthermore the Bank blocked some undesirable websites which holds movies, during the day. However there are no procedures to discipline employees who download unnecessary large amount of data.

v. Train employees regularly

Table 5 shows that 33 respondents out of 55 strongly agreed on the effectiveness of regular employee trainings to protect the company's data while21 respondents only agreed.The view of the majority of respondents regarding the effectiveness of regular employee trainings, lied between strongly agree and agree, with a weighted mean of 4.58. However the standard deviation of 0.534 indicated that respondents are dispersed on their responses.

Additional security measures to be put in place to improve data security

To know whether some measures could be added to the existing security mechanisms, respondents were asked to answer if the following measures might be necessary to the company if added to the existing security system. These measures involved extra security mechanisms such as password and biometric authentication, network monitoring software (i.e Microsoft network monitor, BandwithD, IP Scanner) which could be helpful for network monitoring. Furthermore it involved adding IP tracking techniques, encryption skills for database security and SQL injection tests for the company's website.

Table 6: *Additional security measures necessary to improve data security*

Additional security measures	N	Yes 2	No 1
SQL injection tests	55	44 (80.00%)	11 (20.00%)
Anti-malware	55	4 (7.30%)	51 (92.70%)
IP tracking techniques	55	35 (63.60%)	20 (36.40%)
Password with Biometric authentication	55	29 (52.70%)	26 (47.30%)
Network monitoring software	55	36 (65.50%)	19 (34.50%)

Source: *Field data*

Table 6 indicate that 80.00% who represent 44 respondents out of 55 argued that, SQL injection tests could certainly be useful if incorporated in security system of the company. 92.70% who represent 51 respondents out of 55 argued that Anti-malware softwares could not improve the existing security of the company. Respondents noted that “antiviruses deployed at every endpoint are sufficient and they can do the same job as anti-malwares”. Table 5 indicate that 63.60 % who represent 35 respondents from the total number of 55 argued that IP tracking techniques could be very useful if put in place to improve data security. The majority argued that “IP tracking software should be introduced as a new security mechanism in order to help administrator to analyse history and records of a particular IP address”. Table 5 also indicate that 52.70% who represent 29 respondents acknowledged that password with biometric (Iris and fingerprint recognition) authentication could be very useful to the company if added to the active security system. Generally respondents noted that “using password only to access confidential information is not enough. It is good to introduce new security system such as biometric (Iris and fingerprint recognition) authentication to protect data center”. 65.50% who represent 36 respondents agreed that network monitoring software could be put in place to improve the existing security system. Respondents noted that “these security softwares should be added to the existing information security in order to control network, employees and analyse intrusions”.

Determine how Data Security Levels Affect Online Banking Services Delivery

Multiple Regression Analysis

Multiple regression was used to predict the value of a variable based on the value of two or more other variables. The variable which was to be predicted was called the dependent variable. The variables used to predict the value of the dependent variable were called the independent variables. Multiple linear regression attempted to model the relationship between several explanatory variables and a response variable by fitting a linear equation to observed data.

$Y = b_0 + b_1 X_1 + b_2 X_2 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + b_k X_k + \varepsilon$

Independent variable: X_k, and Coefficient: b_k, Unknown factor: ε, and Dependent variable: Y

Assume that: Y: online banking Service

X_1: computer anti-virus , X_2: firewalls, X_3: digital signatures, X_4: Backup and recovery, X_5: encryption, X_6: physical policy, X_7: motion sensors, X_8: Alarms, X_9: physical guards, X_{10}: disaster plan.

Table 7: *Multiple Regression Analysis Model*

Model		B	Std. Error	Beta	T	Sig.
1	(Constant)	-2.542	2.450		-1.038	.305
	Computer anti-virus	.125	.286	.047	.437	.664
	Digital signatures	1.101	.136	.778	8.077	.000
	Cryptography	.073	.142	.048	.514	.610
	Backup and recover	.108	.162	.070	.670	.506
	Motion sensors	-.617	.233	-.266	-2.646	.011
	Alarm	.015	.143	.010	.103	.919
	Firewalls	.302	.216	.143	1.399	.169
	Physical Guards	.103	.174	.059	.593	.556
	Disaster plan	.202	.133	.154	1.526	.134

a. Dependent Variable: Online Banking Services

Source: *Field research data*

$Y = b0 + b1\ X_1 + b2\ X_2 + b3X_3 + b4X_4 + b5\ X_5 + b6X_6 + b7X_7 + b8\ X_8 + b9\ X_9 + Ɛ$

$Y = -2.542 + 0.125\ X_1 + 1.101\ X_2 + 0.073X_3 + 0.108\ X_4 - 0.617\ X_5 + 0.015\ X_6 + 0.302\ X_7 + 0.103\ X_8 + 0.\ 202\ X_9 + 0.602$ where $Ɛ = 0.602$

The general form of the equation to predict online banking Service from Computer anti-virus, Digital signatures, Encryption, Backup and recovery, Motion sensors, Alarm, Firewalls, Physical Guards, Disaster plan is:

Online Banking Service = -2.542+ 0.125 Computer anti-virus + 1.101 Digital signatures + 0.073 Encryption + 0.108 Backup and recovery -0.617 Motion sensors + 0.015 Alarm + 0.302 Firewalls + 0.103 Physical Guards +0.202 Disaster plan+0.602

***Table 8:** Model Summaries*

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.793[a]	.628	.554	.602

a. Predictors: (Constant), Disaster plan, Motion sensors, Firewalls, encryption, Alarm, Digital signatures, Physical Guards, Backup and recovery, Computer anti-virus

***Source:** Field research data*

The R-squared value, denoted by R^2, is the square of the correlation. It measures the proportion of variation in the dependent variable that can be attributed to the independent variable. The linear correlation coefficient called r measures the strength between two variables. When r is close to 1 the linear correlation is described as strong positive thus the correlation is positive. When r is close -1 the linear correlation is described as strong negative thus the correlation is negative. The study revealed r = 0.793, this meant that there was a very strong positive multiple correlation between independent variables including disaster plan, Motion sensors, Firewalls, encryption, Alarm, Digital signatures, Physical Guards, Backup and recovery, Computer anti-virus and the dependent variable (online banking services). It showed that r^2= 0.628, which meant that 62.80% of total variation in y could be explained by linear relationship between x and y and the remaining total variation of 37.20% was unexplained. This correlation was generally described as strong one.

CONCLUSIONS

Answers to the Research Questions

The research study was carried out to address the following research questions:

1. **How are the root causes of data insecurity at Access Bank, Kigali, Rwanda?**

The main causes of data insecurity at Access Bank are firstly internal based attacks (system users) as indicated by 50.90 % of respondents in Table 1; 58.20% of respondents considered viruses and malicious softwares as the 2nd major cause of data insecurity at the Bank.

2. **How effective are data security measures that are currently used at Access Bank, Kigali, Rwanda?**

In Table 4, the majority of respondents strongly agreed about the effectiveness of a documented policy. However 38.20% of respondents were neutral on the effectiveness of involving users in data security implementationwhile49.10 % of respondents strongly agreed on the effectiveness of the procedures put in place to discipline employees who violate the Bank's policy.

3. **How can are additional security measures be put in place to improve data security at Access Bank, Kigali, Rwanda?**

In Table 5, majority of respondents argued that, SQL injection tests, password with biometric (Iris and fingerprint recognition) authentication company, network monitoring software and IP tracking techniques could be very useful to the company if put in place to improve data security.

4. **How do data security preparedness levels at Access Bank, Kigali, Rwanda affect online banking services?**

In this study the Table 7 shows that a value of r equal to 0.793, indicates a good level of prediction and the coefficient of determination (r^2) equal to 0.628. Therefore there was a strong positive correlation between data securitypreparedness levels and online banking services.

Recommendations

In short term it is recommended to Access Bank to:

1. Provide training to every employee of the Bank on information security, not only to IT employees; as employees work with data and can be easily manipulated if they are not trained.

2. Provide regular assistance to customers in order to avoid identity theft and the revelation of important information on telephone or on email. Meanwhile it is also recommended to customers to learn about identity theft.

Suggestions for Further Study

Based on the problems met through this study more work should be carried out in the future, in the area of data security in order to improve its efficiency.

1. Since the study dealt with data security, future studies should concentrate on the process of database encryption using SQL especially in the context of software used in Banking industry.
2. Being a case study a more general study should be carried out among other banks
3. A long term study (i.e. Longitudinal study should be carried out on the mentioned topic) about the effect of changing technology of data security on financial services.
4. A study should be carried out on the effect of malicious actions against information systems.
5. A study should be carried out on the traceability of persons and goods on the network.
6. A study on the implementation of biometric system in information security should be carried out.

REFERENCES

[1] McLean, J. (1995). The Specification and Modeling of ComputerSecurity. Washington, D.C.: Naval Research Laboratory.

[2] Kitchenham, B. & Pfleeger, S. L. (2003).Principles of Survey Research Part 6: Data Analysis. Class lecture for Software Engineering Course. Keele University, UK.

[3] Kritzinger, E. (2012).A Framework for Cyber Security in Africa. Journal of Information Assurance & Cyber security, 12 (2), 32-51.

[4] Salahuddin, M. A. (2011). Information security management: A case study of an information security culture. Unpublished doctoral dissertation, Queensland University of Technology, Brisbane, Australia.

[5] Stallings, W. (2011). Network security essentials: applications and standards. (4th ed.). New Jersey: Pearson Education.

[6] Stewart, A. (2005). Information security technologies as a commodity input. Information Management & Computer Security, 13 (1), 5-15.

[7] Williams, R. (2007). Introduction to: Basic Security Concepts. A Guide for Administrators and Home Users on the design and implementation of security for your network, 9(14), 50-65.

[8] Younus, A., Qureshi, M. & Arlsan,A. K. (2009). Philosophical Survey of Passwords.International Journal of Computer Science and Information Security, 12(1), 8-12.

[9] Tarushi,S. (2014). Email security using clustering algorithms. International Journal of Computer Science and Information Security, 12(1), 49-54.