DETERMINANTS OF DATA SECURITY IN MANAGEMENT INFORMATION SYSTEMS OF COMMERCIAL BANKS IN NAIROBI, KENYA

BY

JAMES MURAGE KWERI
D53/CTY/PT/20805/2010

A RESEARCH PROJECT SUBMITTED TO THE SCHOOL OF BUSINESS IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE MASTERS OF BUSINESS ADMINISTRATION DEGREE OF KENYATTA UNIVERSITY
DECLARATION

I declare that this is my original work and has not been submitted in any other university or institution for examination.

Signature ___________________________ Date 07/06/2013

(James Murage Kweri) (D53/CTY/PT/20805/2010)

This research project has been presented for examination with our approval as the university supervisors

Signature ___________________________ Date 07/06/2013

Ms Gladys Kimutai
Lecturer, Management Science Department

Signature ___________________________ Date 14/06/2013

John Kandiri
Lecturer, CIT Department, Kenyatta University

This research project has been presented for examination with my approval as chairperson of the department;

Ms Gladys Kimutai
Chairperson, Department of management Science

Signature ___________________________ Date 07/06/2013
ABSTRACT

In Kenya, rarely are cases concerning data security breaches on commercial banks reported or documented. This does not however mean that there are no such cases or that the information systems used by the commercial banks are completely secure. In as much as due diligence and gross assessment of usage, vulnerability, security and recovery of the systems adopted by these banks is done before their adoption, it is worth to note that the human brain has remained superior to computers, implying therefore that the information stored within these information systems is not fool proof and that there do exist risks of manipulation of their data by rogue and systematic users. Further, limited study has been carried out to determine factors that influence data security in the Information systems used by the banks. Occurrence of a breach in data security is unpredictable and as such, informed defence against their occurrence is critical. It is against this backdrop that this study seeks to establish the factors that influence data security in commercial banks. The objective of the study was to determine the factors that influence data security in the management information systems used by commercial banks in Nairobi, Kenya. The study will adopt a cross-sectional survey in which different banks will be studied. Primary data was collected using a questionnaire while an extensive literature review has been done using various secondary sources. The target population was the information security staff working in the headquarters of commercial banks located in Nairobi. A census for all the banks in Nairobi was carried out and the study targeted two respondents per bank, at two strata; one senior IT manager and a general IT technician. Questionnaires were distributed at all the bank’s headquarters and collected after a period of seven days. Introduction correspondence were done through email to all the bank’s human resource department which were requested to allocate two random respondents. The data collected was thereafter coded and entered into SPSS and analysed using descriptive statistics and Pearson correlation. Out of 86 questionnaires distributed 66 were successfully completed and returned by respondents from 34 commercial banks, giving questionnaire response rate of 76.74%. The results indicates that type of data increases chances of breach attempts. The amount of data is strongly positively correlated with data integrity and network security. The study also established that customers have contributed to cases of fraud due to poor handling of their data. Majority of respondents indicated that their organization have experienced frauds through use of hostile technology e.g. ATM skimming. From the research findings, it can be concluded that type and size of data, user knowledge and hostile technology does influence data integrity and network security. The research therefore concludes that both sufficient financial and human resources should be deployed by the commercial banks to deal with data security. This study identifies key factors in banks data that might compromise data security with a view to educating the stewards of banks influencing their direction of designing systems to guarantee banks data integrity and network security. The research recommends that for the integrity of the data and network security the top management should support effective training, skill up-grading and awareness mechanisms to bank employees that would respond and continuously adapt to emerging technological challenges in the bank’s MIS infrastructure.