

**INFORMATION SECURITY AND PROSPERITY OF
MOBILE NETWORK OPERATORS IN KENYA**

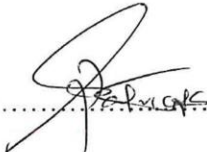
**BY
PATRICK NABWAYO NECHENJE**

**A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT
OF THE REQUIREMENT FOR THE DEGREE OF MASTERS IN
BUSINESS ADMINISTRATION, SCHOOL OF BUSINESS UNIVERSITY
OF NAIROBI**

2019

DECLARATION.

I declare this research project is my original work and that it has not been presented for a degree in any other university or learning institution for examination or academic purposes.

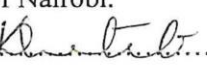
Signature  Date 20/11/19

PATRICK NABWAYO NECHENJE
REG NO: D61/9640/2018

This research project has been submitted for examination with our approval as the appointed university supervisor

PROFESSOR KATE LITONDO

Department of Management Science,
School of Business,
University of Nairobi.

Signature  Date 20/11/19

ACKNOWLEDGMENT

Humbly admit that this success is a culmination of a collaborative process spearheaded by various people who i will forever be indebted to. Wish to convey and express heartfelt appreciation to the following for their steadfast backing, encouragement, and supervision throughout the course. My Project supervisor, Professor Kate Litondo, for her fervent support and professional guidance that shepherded me throughout the entire process. This is a success owed to you. My dad and mum, who tirelessly encouraged me to soldier on with the struggle, their words of wisdom and encouragement miraculously propelled me to extraordinary levels throughout the difficult moments of the research undertaking. We have all triumphed. Lastly, to God the Almighty, for granting me the inner strength, the stamina and mental stability which empowered me to complete the study, this was never be taken for granted. Thank you all.

DEDICATION

The project is dedicated to my cherished parents for their incessant prayers besides aspirations to have me achieve this great milestone. Their abundant, vivid, expressed joy and trust in me will forever be etched in my heart. May the love of God and his blessings be upon their lives.

ABBREVIATIONS

PLC : Public Limited Company

CA : Communications Authority of Kenya

ICT : Information Communications Technology

CIA : Confidentiality, Integrity, Availability.

AA : Appropriate Access.

LTE : Long Term Evolution.

2 G : Second Generation

3 G : Third Generation

4 G : Fourth Generation

5 G : Fifth Generation

MNOs : Mobile Network Operators.

LOIS : Level of Information Security

COIS : Challenge of Information Security

MOIS : Mitigation of Challenges of Information Security

PRO : Prosperity

NPS : Net Promoter Score

ANOVA : Analysis of Variance

TABLE OF CONTENTS

ACKNOWLEDGMENT	iii
DEDICATION.....	iv
ABBREVIATIONS.....	v
LIST OF TABLES	ix
LIST OF FIGURES	x
ABSTRACT.....	xi
CHAPTER ONE: INTRODUCTION	1
1.1 Background of the Study	1
1.1.1 Information Security	2
1.1.2 The Concept of Prosperity	3
1.2 Research Problem.....	6
1.3 Research Objective.....	9
1.4 Value of the Study	9
CHAPTER TWO: LITERATURE REVIEW.....	10
2.1. Introduction	10
2.2. Theoretical Foundations	10
2.2.1 The General Deterrence Theory	10
2.2.2. Integrated System Theory of Information Security Management	11
2.2.3 The Information Security Management Theory	11
2.3 Information Security in Organizations	12
2.4 Challenges of Information Security	12
2.5 Mitigation Information Security Challenges.....	13
2.6 Information Security and Prosperity of Mobile Network Operators.....	14
2.7 Literature Review Summary	15
2.8. Conceptual Framework	16
CHAPTER THREE: RESEARCH METHODOLOGY	17

3.1 Introduction	17
3.2. Research Design.....	17
3.3 Population and Sample for the Study	17
3.4 Data Collection.....	17
CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION	19
4.1 Introduction	19
4.2 Response Rate	19
4.3 Demographic characteristic of Respondents	19
4.3.1 Distribution of Respondent by Gender	20
4.3.2 Distribution of Respondent by Age	20
4.3.3 Distribution of Respondent by Education Level	21
4.3.4 Distribution of respondents by Duration of Employment	21
4.3.5 Distribution of Respondents by Organization	22
4.3.6 Duration of Operation.....	22
4.3.7 Distribution of Respondents by Department	22
4.3.8 Number of employees in Department.....	23
4.3.9 Position Held	24
4.3.10 Role Played by Respondents	25
4.4 Level of Information Security in Kenya’s Mobile Network Operators	25
4.5 Challenges of Implementing Information Security of MNOs’ in Kenya	27
4.6 Mitigation of Information Security challenges in Mobile Network Operators in Kenya	28
4.7 Prosperity of Mobile Network Operators in Kenya	29
4.7.1 Financial Target	29
4.7.2 Innovations	29
4.7.3 Net Promoter Score (NPS)	30
4.8 Effect of Information Security on Prosperity of Mobile Network Operators in Kenya.	30
4.8.1 Regression Analysis	30
4.9 Discussion of the Findings	33

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS	36
5.1 Introduction	36
5.2 Summary of the Findings	36
5.4 Recommendations	37
5.5 Limitation of the Study	38
5.6 Suggestion for Future Research	38
REFERENCES.....	39
APPENDICES	42
APPENDIX 1: QUESTIONNAIRE.....	42

LIST OF TABLES

Table 4.1: Response Rate	19
Table 4.2: Distribution of Respondent by Gender	20
Table 4.3: Distribution of Respondent by Age	20
Table 4.4: Distribution of Respondent by Education Level	21
Table 4.5: Distribution of respondents by Duration of Employment	21
Table 4.6: Distribution of Respondent by Organization.....	22
Table 4.7: Duration of operation	22
Table 4.8: Distribution of respondents by Department	23
Table 4.9: Number of Employees	23
Table 4.10: Position Held	24
Table 4.11: Role Played.....	25
Table 4.12: Level of Information Security	26
Table 4.13: Challenges of implementing Information Security	27
Table 4.14: Mitigation of Information Security challenges.....	28
Table 4.15: Financial Target.....	29
Table 4.16: Innovations	29
Table 4.17: Net Promoter Score	30
Table 4.18: Model Summary	31
Table 4.19: ANOVA.....	31
Table 4.20: Model Coefficients	32

LIST OF FIGURES

Figure 2.1: Conceptual Framework.	16
--	----

ABSTRACT

Information security is ultimately regarded as protection of information from any unapproved access or consumption, interference, modifications or damage whilst ensuring its confidentiality, integrity and availability. Regarded as an organizational asset, information remains the most sought for and guarded item in any prospering organization. The prosperity of the mobile operators has been related to various activities operationalized within, the key to all, the part information safety shows in determining flourishing of respective organizations. Information security plays a pivotal role in driving organizations to prosperity which generally refers to a situation whereby the organizations in context continue to experience general wellbeing with the display of progress and fulfillment of its vision not just wealth. Prosperity continues to evade organizations that have disregarded the importance and essentials of safeguarding information. The purpose of this research was to determine information security effects on the prosperity of Kenya's mobile network operators namely Safaricom PLC, Airtel Kenya, and Telkom Kenya LTD. Generally, the study aimed at determining how Information Security has influenced the prosperity of Kenya's mobile network operators at large .Specifically the study was to firstly establish the level of Information Security in Kenya's Mobile Network Operators, Secondly determine challenges of implementing Information Security of Kenya's Mobile Network Operators, thirdly, find out the extent of mitigation of Information Security challenges in MNOs' in Kenya, and lastly investigate the consequence of Information Security on Prosperity of MNOs'. The study employed a descriptive research design that gave the required quantitative answers with reduced prejudices hence giving a correct representation of essentials. The study found out there is a great level of Information Security implementation among MNOs in Kenya. Despite the success in this front, MNOs lack information security policies at the departmental level. Further, the study established that Mobile Network Operators face limited challenges during the carrying out of information safety however, complexities of security attacks remain a major challenge experienced by MNOs in Kenya. The Study did find out that that MNOs' in Kenya mitigate information security challenges to a great extent through various ways, of interest to note was that adoption of core practice deliveries through enhanced training, development, policies enhancements are not highly adopted by MNOs in Kenya. Finally, of great importance, the study found out that Information Security positively affects the Prosperity of Mobile Network Operators in Kenya. Key to these findings, this research is expected to motivate the mobile network operators to improve their existing information security frameworks and strengthen the existing infrastructure in terms of adopting the most suitable and better ways of managing information security. Policymakers will find the study reliable and helpful in policy and strategy formulation for information security, academicians, scholars, and future researchers will benefit from the conclusions and commendations as it would form a basis of foundation and reference for further improvement.

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Information is a valued asset of any organization which should be safeguarded and preserved (Rao, 2010). Viewed as processed data in a meaningful form including business information that is warehoused, is in transit, though in a raw or unrefined state. The information available on computer networks, printed or locked in file lockers, has been the most vulnerable and sought item confirming the importance of information security as critical to organizations (Ataya et al. 2006). Successful driven enterprises have recognized the importance of information security, for them to achieve their goals, strategies ought to be crafted to compete for the cut-throat competitive markets (Mujtaba, 2010). Over the past century, organizations have implemented information systems for managing their business process making information security a continuous concern (Stalling & Brown 2008). Enhancement of the security measures is the protection of organization assets that reduce the chances of being victimized by intruders (Stalling, 2008). In recent times, organizations have been compelled to review their information collection and handling practices due to serious threats exploitable by the intruders (Rivard, 2014).

Various theories have been fronted to explain the Information Security Prosperity phenomenon. The General deterrence theory by (Cohen & Nagin, 1978) premised on the three components of severity, certainty and celerity postulates controls to serve as the deterrent mechanism for information system misuse. The theory advocates for mechanisms that could be initiated to arm the providers against increasing risks. On the other hand, Integrated System Theory by (Chi, Chao & Tang, 2003) postulates the need for an integrated approach in understanding information safe keeping and its managing strategies. In understanding the information security and prosperity phenomenon, the theory envisages the numerous security challenges prevailing and thereafter lay a foundation to establish a mitigating framework. The other theory Information Security Management Theory by (Finne, 1998) has been used in the study to bring out the importance of controls and processes on information security. The models acknowledge aspects of an in-depth understanding of business processes and controls in the management of security. Mobile telephony industry has become

part of the expansive converged industry offering services and products that now handle the growing quantity of data and information, offered services like data, voice, mobile money and much other value-adding services are a reflection of the numerous amounts of sensitive information the operators have a responsibility to safeguard. Safaricom PLC, Airtel Kenya, and Telkom Kenya handle large quantities of data and sensitive information which not safeguarded may lead to business catastrophes in terms of hefty fines and loss of subscribers. The sector has exponentially grown in Kenya with licensing of three mobile network operators, Safaricom PLC, Airtel Kenya, and Telkom Kenya. Safaricom PLC is the largest mobile service provider followed by Airtel and Telkom Kenya respectfully.

1.1.1 Information Security

Scholars have defined Information security differently. Others have defined information security based on two standards, the Classic C-I-A and New AA standards. The Classic C-I-A standard outlines Information Security as confidentiality: integrity: and availability of facts (Gupta, 2015). Referred to at times as the C-I-A triad. New AA standard defines Information Security as giving appropriate access to every fragment of information (Gibbard, 2003). According to Nissenbaum (2005), the definitions are designed models for guiding information security policies. The AA access standard captures information security based on incident segregation verification and is uncluttered and flexible while on the other hand classic CIA based on the chord is cluttered and inflexible. Generally, Niekerk (2013) states that computer security, information security, and cybersecurity collectively is the security of computer systems aimed at ultimately achieving the safety of the information resources. Further regards Information security as once a purely technical phenomenon converted over time to match the technological evolution. Information security is, therefore, a way in which human capital in organizations use available provisions of information to apply suitable controls aimed at protecting information from threats (Kukkonen, 2007).

Owing to a large amount of data being dealt with, information security has gained more interest in organizations and as such, an online transaction increase, and lack of security awareness have become greater motivations to exploit the software and human vulnerabilities (Santos, 2016). Physical Security risks organizations have to

deal with are, terrorism attacks, deluges, fires earthquakes and tremors. According to (Pereira, 2016) a serious impact on business profitability, reputation, customer satisfaction, confidence, and economic growth can be a consequence of theft and loss of organizational information. According to Acosta (2016), the fastest-growing information crime is identity theft which involves loss of customer vital data. Enterprises are faced with threats perpetrated by insiders with clear malicious intent and unintentional likely human error (Malik, 2004). External breaches aided by insiders pose as the most damaging information security risk challenge due to the inherent vulnerability existing in the security framework.

This study will adopt the AA characterization as it presents broader categorization which is extensionally and intentionally adequate, and helpful in the analysis of information security. Over time studies have continued to suggest and front for the adoption of other alternative definition models due to presented inadequacies and identified problems of the existing classic standards (Pieprzyk, 2003). (Gibbard 2003) opines that besides the three facets of the classic standard, other factors ought to be considered and proposes the expansion of the triad to include control, integrity, authentication, availability, and Utility. It is observable that more scholars are of the view new definition AA standard should be adopted as it achieves and captures the notion of information security compared to other characterization fronted (Chopple, 2005). According to Pieprzyk(2003), the broader categorization manifested in the AA standard captures the sense of the concept and provides a more realistic scope. (Lundergreen, 2003) affirms that this standard recognizes the existing contextual variation of security needs and incorporates the softer issues of information security.

1.1.2 The Concept of Prosperity

Various scholars have defined prosperity differently, going by Stiglitz (2009) prosperity is the art of flourishing accompanied with good fortunes, successful social status, and encompasses not only wealth but other factors independent of wealth such as happiness and health. Others have defined prosperity as the general wellbeing with a display of progress and fulfillment of all wishes, not just wealth (Randall 1998). Prosperity has largely been defined regarding humans, entities and economic wellbeing of nations and countries. However going by (Mamford 2003 & Kilpatrick,

1992) there is an emerging belief that portrays the prosperity of organizations in light of growth, accomplishments, benefits, boom, expansion, growth, success, abundance and advantage. Prosperity creates a unique display of characteristics and indicators are used to realize a change in a normal or desired state providing information on preset objectives (Askounis, 2015). Scholars (Markou, Kokkinakos, & Markaki, 2005) describe prosperity indicators in a landscape analysis as a metric of weighing the level of prosperity in modern groups, they classify the prosperity indicators into economic and social indicators. According to the Greek scholars (Kokkinakos & Prastakos 2015), the indicators provide information on the financial or social standing of organizations while indicating shortcomings and weaknesses. (Tangen, 2004) postulates that social indicators play and measure changes in social concern and also serve numerous objectives related to prosperity and growth.

This study intends to adopt both the social and economic quantified and qualitative indicators as they will adequately offer insights on sustainability, growth, and satisfaction. The set of economic indicators that have been associated with mobile service providers in Kenya are financial indicators like revenue, budget deficits, and expenditures. The majority of the scholars opine that prosperity analysis needs to go beyond economics and finance to incorporate the social aspect and to bring a new understanding of the intricate system alongside expounding views and increasing responsibility (Sterman, 2000).

Safaricom PLC, Airtel Kenya, and Telkom Kenya all have obligations to fulfill growth targets, make their customers happy and compound their services with innovations to ultimately bring fulfillment to their respective organizations. The ultimate prosperity indicators the mobile service providers will be striving to achieve, will be the wellbeing of the service providers indicated by harmony, and identity within the organization, self-respect, wealth, longevity of their business and social relationship as described by (Kokkinakos 2005). Prosperity in organizations is thus achieved when organizations are seen to serve the needs of their customers with intense dedication (Baptista, 2016). They tend to rapidly deploy new products offering superior value to their target markets ultimately achieving their business goals (Tuppen, 2007)

1.1.3. Mobile Network Operators

Kenya's mobile telephony sub-sector has over the past exponentially grown. Kenya's Government acknowledges the importance of information and communication sectors to its economic development. This study will focus on the three MNOs' in Kenya, Safaricom PLC, Airtel Kenya, and Telkom Kenya. Safaricom began as mobile department within Telkom Kenya in 1997 and enhanced demand for mobile cellular phone connections. Airtel Kenya joined the foray in the year 2000. The three players embarked on countrywide cellular expansion mission of their services triggering a fierce competitive war in the market translating to an expansive extension of mobile network footprint in rural and urban areas of the country.

Safaricom PLC is a listed company founded in 1997 as a mobile network operator. The company is largely owned by Vodacom South Africa and the Government of Kenya. The organization offers converged services of voice, data, and mobile money transfer services popularly known as M-PESA. It has a workforce of over 5000 employees distributed across its regionalized structure in the country. On the technological front, the operator provides the 2G, 3G, 4G, LTE technologies and is in the process of launching the 5G technology. Safaricom PLC has a subscriber base of over 30 M subscribers and prides in transforming lives. Relevance to the study, is by virtue of its strongest and widest mobile network coverage in Kenya providing wide range of services and connecting networks worldwide, the company possesses and processes massive quantities of data and subscribers material which demands safeguarding and protection. As a technological leader, Safaricom PLC remains a key target of cyber and information intruders hence prompting adeptness to minimize information systems risks through an enhanced level of combative, and neutralized attacks.

Airtel is the second-main mobile operator in the country, founded in the year 2000. The parent organization is Bharti Airtel of India. The operator has a subscriber base of over 9 million subscribers providing a variety of services in voice, data and mobile money transfer services popularly known as Airtel Money. Organizational structural changes over the past years have seen the company change its management team, transitioning from Kencel communication to Celtel then Zain before rebranding to Airtel Kenya in 2010. The operator has a nationwide mobile network footprint and

provides the 2G,3G services, recently launched the 4G services. As an operator, it connects networks worldwide through a range of its systems and services and continues to contribute positively to the economy of this country.

Telkom Kenya is the third largest but oldest operator in the country, founded in the year 1999 as Kenya Post and Telecommunication Ltd which began as a fixed-line operator before venturing into the mobile telephony services to offer the 2G and 3G technologies. It has over 1400 employees spread across the country with a subscriber base of over 4Million and contributes positively to the economy of the country through the various services it offers. It prides itself on its money mobile transfer services popularly known as T-KASH.

To warrant the study, issues of concern are anchored on what mobile technology offers in the dynamic domain of the Information Communication Technology environment. The offers remain largely similar but fundamentally distinct to each operator prevail and continue to present challenges. (Bulut, 2007) .The operational environment and space having been opened up to allow the players into the market to drive technological investments. The technological advancements have given rise to increased innovations impact, this remains an issue of concern (Khadraoui, 2008). Utilization of these technologies by mobile operators to reach a wider audience safely and securely has remained an issue of concern for the operators. Introduction of online services riding on mobile networks, internet services and mobile payments services, payphone online services remain a potential risk to businesses when not well secured according to (Darwiche, 2018. The notion of having a compromised network has become a sure way of obliterating the network providers and that becomes a sure way of their commercial demise inferred (Mouilin, 2002). Cutting edge technologies that become vulnerable overtime presents concerns warranting the study (Bauwman, 2008).

1.2 Research Problem

Information insecurity leads to societal chaos manifested in strife, disobedience, expensive suits and instability (Argarrwal, 2009). These factors are limiting and retrogressive to the growth of organizations states (Triana, 2011). The rapid growth of

information translates into improved services which enhances the prosperity of organizations at the same time posing security threats to the operations of entities (Karjaluo, 2005). The information and communication journey of mobile network operators driving on technology is change based owing to the high levels of innovations and the ability to craft strategies and approaches for varied use across. The important role of the economic development and growth played by the mobile network operators cannot be undermined. Mobile network operators have to renew their approach towards safeguarding information in the digital revolution (Tompuri 2014). Ismail (2015) suggests, as a result of increasing risks, mechanisms and strategies must be put in place to minimize the effects.

The problem appears to be in the capacity and pace at which mobile network operators are balancing the worrying issue of information security and prosperity. Real struggles to mitigate the risks regardless of the price they have to pay to flourish, and to implement workable strategies which may be lacking exist. While the attacks are against the most dangerous risks faced by the operators, deployed techniques by the information criminals are alarmingly evolving yet many operators and organizations continue to rely on past ineffective security technologies for present and future threats. According to (Gemalto, 2015) breach erodes customers' trust and leads to operational paralysis of many organizations. The study dwells more on the impacts of breached information security and generally the resulting consequences. A 2014 Consultancy study done in Canada on Security and Prosperity determined that the achievement of the long term prosperity and improved competitiveness relied on the safety of the critical enablers. The study demonstrated the need to have a security system that would ensure greater achievements, the merits of the study could not however underpin information security to prospering organizations. The 2016 Intelligent, and Security reform study done in Australia, regarded mobile networks and systems as critical facilities and infrastructure vital to the delivery of other sectors services. The sector acted as a backbone of other sectors. According to the study, a compromised mobile network would therefore, have a significant ripple effect on other critical infrastructure sectors ultimately impacting the Kenyan economy.

The critical vulnerabilities created within the mobile network operators arise from internal and external environments. In Kenya, it is not sufficient in an environment

with large numbers of service providers who interact globally with a commercial interest to align and strengthen their security needs. Kahonge (2009) agrees to the information technology security practice analysis done in Kenya which established that organizations regardless of size significantly relied on open information and communication technology for optimal performance of the business. He acknowledges the thriving digital economy but decries information on the hand had become a vulnerable business asset demanding protection. Going by Kahonge (2009), mobile network operators are thus urged to investigate and establish a protection mechanism as attacks become more complex and uncertain. Osido (2015) argues that very little may be done to avert worsening the situation if attention is not paid to the valuable areas as the systems remain in the viewable field of criminals. Telkom Kenya through increased risk assessment and development of security programs focuses on information crime, capacity management, and awareness drives internally. The information and prosperity at Airtel Kenya project one better managed through corporate relationships with the highest information security risks relying on the implementation of security regulations. This according to (Serianu, 2015) is a result of an increased motive to a crime that is hurting business gains. (Stanton, 2001) agrees that the industry has strong incentives to safeguard against the arising risk and the security needs are disproportionately spread across the industry.

Although different studies on information security and prosperity exist, few studies did link information security and prosperity. Studies done in Kenya by (Osodo & Kinyanjui, 2015) all established that information and data are fortified through mechanisms of risk assessment and development of security. This largely focused and acknowledged the mechanisms and ability to preserve, protect, without underpinning the effects on prosperity. On the other hand, a study by (Kahonge, 2005) establishes a weak correlation or association of information security and prosperity, it emphasizes reliance of open information and communication technology for the optimal success of their business. The scholar suggests a look into the monetary value of the caused loss. (Kisaka, 2015) agrees and acknowledges information security as being key to organizations' credibility through relatively focusing on the successes of the organizations at large. Other studies done outside Kenya mostly emphasized the technical hard issues of information security, therefore failing to incorporate the soft issues which are likely to impact prosperity (Niekerk 2013). Many studies failed to

develop a comprehensive understanding of the phenomenon associating prosperity with information security, as such the implication dimensions of information security on the prosperity of mobile network operators are yet to be known or established. The studies on Intelligence and Security (2016) appeared to establish a correlation between security and prosperity of telecommunication operators, however, it dwelt more on the rationale of security reforms, risks, and mitigations strategies. In as much as the cited studies seem to agree about the significance of information security, they largely fail in associating it with prosperity. As such, they not only fail to develop a comprehensive understanding of the phenomenon, but also fail to concentrate on the inherent information security levels and challenges organizations face when implementing security policies. The studies also failed to directly link information security to prosperity. This study will attempt to fill this knowledge gap through answering the subsequent research question, How have Information Security influenced the Prosperity of the Mobile Network Operators at large?

1.3 Research Objective

Objective of the study is specifically to

- i. Establish the level of Information Security in Kenya's Mobile Network Operators.
- ii. Determine challenges of implementing Information Security of Kenya's Mobile Network Operators.
- iii. To establish the extent of mitigation for Information Security challenges in Mobile Network Operators in Kenya.
- iv. Establishing the effect of Information Security on the Prosperity of Mobile Network Operators in Kenya.

1.4 Value of the Study

This research is anticipated to inspire mobile network operators to improve their existing information security frameworks and strengthen the existing infrastructure in terms of adopting the most suitable and better ways of the governance of information security. Policymakers will find the study reliable policy and strategy formulation. The study will enrich, improve and add knowledge on information security and prosperity at large. To academicians, scholars and future researchers, the study would form a basis of foundation and reference for further improvements on the subject.

CHAPTER TWO: LITERATURE REVIEW

2.1. Introduction

This section reviews the theoretical foundation of the relationship between Information Security and Prosperity.

2.2. Theoretical Foundations

Concepts have been fronted to elucidate the Information Security and Prosperity phenomenon. Three theories will provide the basis for this study: The General Deterrence Theory, The Integrated System Theory, and Information Security Management Theory. The theories are deliberated below.

2.2.1 The General Deterrence Theory

The General Deterrence Theory (Cohen & Nagin, 1978) fronts that definite controls are able to function as a limiting mechanism by aggregating the perceived threat of reprimand for information system abuse. The concept, posits consumer responsiveness of information safety countermeasures, openly impacts the observed conviction and severity of organizations prohibitions associated with information system misuse, most importantly reducing misuse intent. The outcomes submit that practices that discourage information abuse are consumer consciousness of security, guidelines, security training, and computer expertise. It further suggests that the seeming rigorousness of authorizations is further effective in decreasing information exploitation compared to certainty of sanctions. The effect of sanction perception varies based on the depth of morals. In an ideal situation, this theory advocates methods of punishment intended to deter misuse or any unethical behavior toward information security. It projects human propagation of rational calculations before indulgence into acts that may amount to a misuse of the information.

As such, this concept can leverage the merits of the theory which on the other hand determines threats likely to undermine the prosperity of the operators. The attitude towards information security has been shaped by a possible predetermined output which tends to determine whether an organization will spur or stifle growth. Evaluation of the information security risks and determination of the expected outcome largely influences attitude towards the wellbeing of the organization. The

theory captures the ethical exuberance concerning the existing information security governance structures. In the country, it reflects upon the basic fundamental human intentions expected towards embracing measures that will ensure data safety and prosperity.

2.2.2. Integrated System Theory of Information Security Management

Integrated System Theory of Information Security Management (Chi, Chao, & Tang, 2003) on the other hand postulates the merits of combined system theory in undertaking information safety management approach and management outcome fixes. The theory explores the very many unprecedented security challenges faced by organizations and decries a lack of security management frameworks. It proposes combination of risk, contingencies, auditing and management policies theories to build a comprehensive theory of Information Security Management.

The theory advocates for a more unified and management approach in handling information security issues holistically. Relevance to the study is premised on the very many unprecedented security challenges organizations and operators are facing, and the relevant approaches adopted to ensure information is managed in the most effective ways to prosper institutions. The domain of information systems presents a strategic problem that remains a challenge for most senior managers (Clarke, 2012). The Integrated System Theory fronts for softer approaches towards strategic thinking in information systems.

2.2.3 The Information Security Management Theory

Information Security Management Theory (Finne, 1998) discloses the wider complexities of an interdisciplinary nature, which highlights the information of having an adequate understanding of many concepts of information security risk management. The model identifies critical business organizational processes and internal controls of information security risk management. The model, articulates how business processes are a foundation of prosperity in those organizations that uphold information security by injecting the aspect of an in-depth understanding of the business process and controls. Eloff & Eloff (2003) stated that the optimal way to combine products and processes for information security is by defining a code of practice during the evaluation process. Solms (2004) identifies key aspects to avoid

mistakes and serious errors in the evaluation process of information security management from different viewpoints. The scholars view information security as an organizational responsibility and regard data protection as a business issue rather than a technical problem.

2.3 Information Security in Organizations

Going by Fenz (2014) the critical concern of information security is to guarantee business continuity at controlled risks and minimized impact. Information technology has presented major security challenges affecting organizations in many ways through Internal and external threats, as such securing generated information from external attacks has become very important (Baxter, 1999). According to the Ground Breaking Global study, lack of human capacity, training, and board room prioritization have resulted in increased information security incidents extending to ciphering, access rights and control, Intrusion detection, proxies, authentication, and firewalls. To establish the biggest risk an important assessment is performed (Vijayan, 2002). According to Parker (1988), the objective is to ensure the essentials of the objects remain uncompromised. As an important aspect of information security, this categorizes security concerns into first-order issues directed against systems such as calamities, the unpredictability of software, and computer abuses. Second-order issues affect the organization's adaptability and flexibility (Scolar, 1988). The safeguards are a burden as they constrain organizational structures and present information security concerns as an elusive issue (Ncumann, 2004).

2.4 Challenges of Information Security

The easiness of access information and digital data belonging to the organization has resulted in serious challenges faced by many organizations. Proving the contributing factors to the security challenges remains key (Fenz et al., 2014). The challenges are regarded as significant issues. Broadly, the challenges can be grouped into people, and access control, with people inadvertently doing things they should do, or not, or not having proper access control on a system (Snekkenes, 2018). Maynard (2016) suggests that intelligence to drive and manage information security systems is derailed by lack of leaders with strong, broad command, and solid background in the field able to pull together a formidable team of security, the problems and threats have become unmanageable, Koyuncu (2018) agrees that skilled staff shortage has also

resulted into decreased numbers of skilled security personnel. Failure to develop security enforcement skills other than traditional information technology has been viewed as a major challenge (Ahmad, 2017). Limited visibility of own environment has posed as a challenge that denies organizations the ability to better manage information security (Spagnoletti, 2008). Misaligned goals within the organization remain a challenge. Otology (2005) decries challenges of budgetary constraints and funding required for the security infrastructure, legislation and industry regulation, identification of quality controls has not been at par with the development of security policies. The enormity of data available makes it difficult to manage and review (Martha, 2005). Failure to prioritize information security increasing vulnerabilities as the essential areas are left out (Johansson, 2005). According to Shahibi (2011) apart from technology failing, the people entrusted with the process have stood out as the perpetrators or proponents of corrupting the system. Vulnerabilities being kept a secret from users leads to a false sense of security (Sauerwein 2017). Mistrust amongst the users violating rights to know and access sought information remains a challenge. (Khan, 2016).

2.5 Mitigation Information Security Challenges

Due to their respective vast networks and potential risks and challenges, mobile network operators have armed themselves by putting in place structures and strategies to mitigate the attacks (Ismail 2015). Williamson (2015) stated that attacks against the operators were a result of what they possessed. Safaricom PLC has adopted appropriate security solutions by layering security layers. The operator has strengthened threat visibility by deploying real-time context threat awareness analytics as a business should be in a position to detect all threat types to prevent information theft. Effective measures ensure business continuity, adoption of decentralized architectures matching the growing traffic enhances the user experience (Gregor, 2007). There is some level of operator infrastructure incorporated into the global network for purposes of quicker recognition of malicious activities on the broader information security ecosystem (Ismail, 2016). Management of information risks requires adeptness to combat and neutralize the attacks (Geer, 2001). The operator has boosted its information security budget and aligned its security plan programs with its business strategies and overall spending. Information security has developed into a fundamental section of the business not just an information

technology challenge (Hiton, 2013), sharing and communicating to improve security while collaborative initiatives carried to gain intelligence on threats (Bidgoli, 2006).

Airtel Kenya has a comprehensive process that also secures its mobile network operations against threats, it has deployed hardening solutions against the threats and bolstered its intelligence-gathering capabilities. Incorporation of the asset management tools and robust intrusion detection tools. The adoption of the awareness of action consists of precepts that see security as a business imperative (Gartner, 2017). Technological safeguards and effectiveness vary from one operator to the other, Telkom Kenya Ltd relies on a mobile device management technology that improves oversight through timely security updates to its mobile devices. Telkom Kenya has streamlined clarity on acceptance user policies, password management policies have been enhanced alongside the application of the two-factor access authentication. A robust software updating and patching process to remediate the risks internally and externally. The three operators have commonly intensified skill development training campaigns, intensified background checks during hiring screening, checks on user rights. Comprehensive policies that have ensured positive behavior and guided the mitigation efforts are in place.

2.6 Information Security and Prosperity of Mobile Network Operators

From a study Challenges and Research direction done in Colorado by (Rees and Grimaila 2007) management of information security largely relies on technical control, even though the study agrees that neither is the business control on its own adequate, it suggests focusing beyond technical and business controls to adopt newer theories and multifaceted approaches to address information issues ravaging enterprises. According to the study, information security management, and activities should primarily concern strategy, and be driven by organizational objectives to warrant action taken, and to support the organization's mission (Blakey, 2001). In contribution to the study, Pipkin (2000) opines that organizational goals will be achieved through the technical, legal and business processes. The Harnessing Information and Technology study by (Tallerro & Gaudette 2010) concurred that the revolutionary changes in Information technology have reinforced the economic and social standing of businesses and society.

The study acknowledges that the ultimate mission of harnessing information for its mission is to eradicate poverty and sustain economic development more so for countries that are still adjusting to the information economy. It further asserts, to achieve the goals, information policies and strategies should be designed and projected at both national and sector levels. A study Information System effectiveness in small businesses by (Hunter & Kelly 2005) done in Singapore evaluated the importance of managerial support for Information system successes, a healthy information system is one that has a strategy with standards and principles, indicators, data sources, and secure as it fulfills the triad of confidentiality, availability, and acceptability, the study showed that both managerial and vendor support are important for an effective information system that contributes to the goals of the business. The study asserts that contribution to the specific business goals through a healthy information system requires the concerted effort of the management and relevant parties. Achievement of business goals will largely contribute to the wellbeing and prosperity of organizations.

2.7 Literature Review Summary

The General Deterrence Theory, The Integrated System Theory of Information Security Management, and The Information Security Management Theory are used to explain the linkage between Information Security and Prosperity. Evaluation of the writings linked to Information Security and Prosperity depicts the importance and relevance of information security at large in an information-driven organization. As shown in some studies and opinion surveys the uptake of this importance is very discouraging, however, the management of many organization have begun appreciating and viewing information security as a key organizational asset (Straub, 1989). Many studies on information security have focused on adoption and development depicting the infancy nature of the uptake on the importance of information security by many organizations (Morris, 2006).

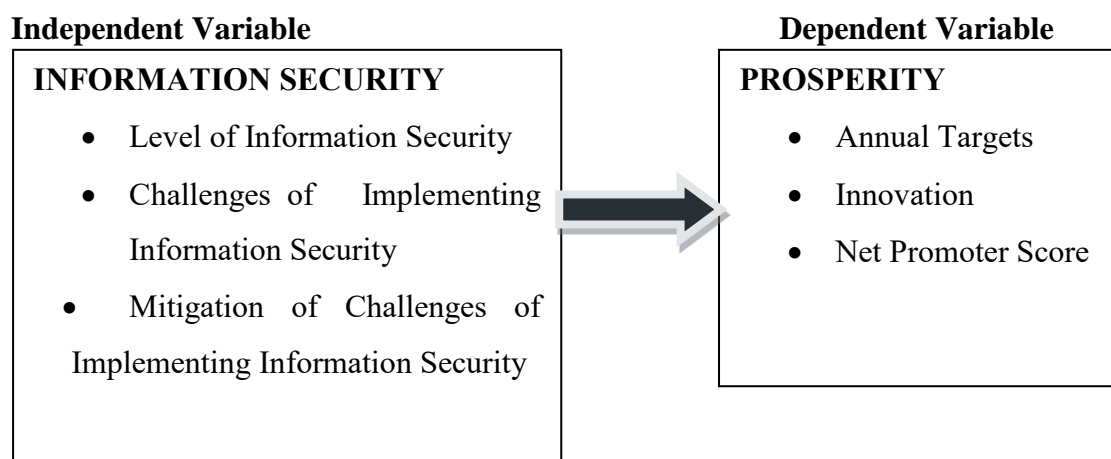
Organizations are reconsidering their security posture by realignment of information security priorities and goals tuning them with organizational objectives at functional levels. This study further illustrates the damage likely to occur from the information breaches and publishes improvement opportunities in security management. Surveys have shown the growing concern the little attention information security continues to

receive from the top management. Studies in the USA by (Kankanhalli, 2003) indicate the infancy level of information security discipline and confirms the existence of little empirical study conducted establishing poor information security practices and prosperity within many organizations. The study advocates for a new conceptual lens by which information security can be observed. Studies have validated the effectiveness of organizational functions as impacted by disharmony between the roles and the senior management (Magal, 1988).

2.8. Conceptual Framework

This framework is used to make a conceptual distinction and organize the ideas establishing the existing association between Information Security and Prosperity as shown in

Figure 2.1



From Figure 2.1, it is clear that there exists a relationship between the independent and dependent variable. Prosperity can be viewed to depend on Information Security. In other words, MNOs' in Kenya may attribute their Prosperity to Information Security. The framework zeroes in on the various determinants and factors of Information Security that influence or determine Prosperity of the MNOs' in Kenya and consequently, positively contributing to the significance of the study.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlines the research methodology applied in conducting the study. It outlined the Research Design, Population, Data Collection and Data Analysis.

3.2. Research Design

Research design is the art of determining appropriate methods to answer asked question, it is an effective strategy providing a structure gathers, collects, and examines data (Sanders, 2009). This study employed a descriptive research design. Going by (Macleod, 2009) descriptive designs give the required quantitative answers with reduced biases and reflecting things in their usual background. It therefore, gives the correct picture for elements under this study at maximized reliability and reduced biases. The design was chosen as it is ideal when a need for organizations analysis, people settings is to be carried out.

3.3 Population and Sample for the Study

Population is the total number of groups, households, elements and individuals, an analytical group for which reliable data is sought (Schindler, 2003). The target respondents for this study will constitute and be limited to the Technical staff of the departments actively responsible for network operations in the three Mobile Network Operators since the information security risk exposure is high amongst these employees. They are also directly accountable in various roles they play in their organizations. The target population for the study was 95 employees, in Safaricom PLC, the population size of technical staff involved in Network Operations is 45, and Airtel Kenya has 27, while Telkom Kenya has 23 employees respectively. The researcher adopted a census method to include all the population in the sample.

3.4 Data Collection

Original data or findings gathered by the researcher is Primary data (Hanoka, 2011). The Study consumed primary data. The primary tool for data collection was self-administered structured questionnaire developed by the researcher and contained open and closed ended matrix questions for quality and value assurance. A Likert scale five point rating was used for each study variable

3.5 Data Analysis

Questionnaires from the field were subjected to the mandatory data management process of consistency evaluation checks, cleaning, coding, entry and finally analyzed using SPSS. The first three objectives of the study were analyzed using mean, standard error and standard deviation. Objective four was solved using regression model formulae below.

$$\text{Regression model: } \mathbf{Y} = \alpha_0 + \alpha_1 \mathbf{x}_1 + \alpha_2 \mathbf{x}_2 + \alpha_3 \mathbf{x}_3 + \mathbf{e}$$

Whereby:

$\mathbf{Y} = \mathbf{PRO}$ = Prosperity.

α_0 = constant.

α_1 , α_2 and α_3 = Regression Coefficients.

$\mathbf{x}_1 = \mathbf{LOIS}$ = Level of Information Security .

$\mathbf{x}_2 = \mathbf{COIS}$ = Challenge of Information Security.

$\mathbf{x}_3 = \mathbf{MOIS}$ = Mitigation of Challenges of Information Security.

\mathbf{e} = error term.

Substituting the above parameters, the regression equation becomes:

$$\mathbf{PRO} = \alpha_0 + \alpha_1 \mathbf{LOIS} + \alpha_2 \mathbf{COIS} + \alpha_3 \mathbf{MOIS} + \mathbf{e}$$

CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents the findings of the study that was carried out to establish the effect of Information Security and the prosperity of Mobile Network Operators in Kenya. Prior to the data analysis, the collected data was entered into SPSS, then checked against data outliers, errors, missing values to ensure the data was well distributed or normal.

4.2 Response Rate

The sample size of this study was 95 employees distributed in the three Mobile Network Operator. The researcher distributed 95 questionnaires, 77 were completed, returned then analyzed representing a response rate of 81.05%. Table 4.1 illustrates response rate. Mugenda & Mugenda (2003) postulates that a response rate of 50% is acceptable for analysis and reporting. Therefore the response rate for this study was excellent and sufficient for data analysis and interpretation.

Table 4.1: Response Rate

Response	Frequency	Percentage
Response	77	81.05
Non Response	18	18.95
Total	95	100

Source, Research data (2019)

4.3 Demographic characteristic of Respondents

Demographic information was presented in the form of frequencies and percentages. This information was vital for the researcher to ascertain the background of the respondents towards their ability in responding to the study variables on the effect of Information Security and the prosperity of Mobile Network Operators in Kenya.

4.3.1 Distribution of Respondent by Gender

The researcher asked this question to establish gender parity and respondents inclusiveness. Table 4.2 represents the findings.

Table 4.2: Distribution of Respondent by Gender

	Frequency	Percent
Female	22	28.6
Male	55	71.4
Total	77	100.0

Source, Research data (2019)

Table 4.2 shows that 55 out of 77 respondents are male and 22 are female. This presents 71.4% and 28.6% in that order and this implies that majority (71.4%) of MNOs employees are male.

4.3.2 Distribution of Respondent by Age

The researcher asked this question in order to establish age of the respondents. The findings are presented in Table 4.3.

Table 4.3: Distribution of Respondent by Age

	Frequency	Percent
24 to 27	7	9.1
28 to 31	15	19.5
32 to 36	35	45.5
37 to 41	10	13.0
Over 41	10	13.0
Total	77	100.0

Source, Research data (2019)

Table 4.3 shows that 7 out of 77 respondents are between 24 and 27 years, 35 are between 32 and 36 years and 15 are between 28 and 31 years. This represent 9.1%, 45.5% and 19.5% in that order. It is also clear from the findings in table 4.3 that 10 out of 77 respondents are between 37 and 41 years and another 10 are over 41 years. This represents 13.0% and 13.0% in that order. The findings infer that the majority (87%) of the MNO employees are below 41 years.

4.3.3 Distribution of Respondent by Education Level

The researcher asked this question in order to establish the respondent's education level. The findings are presented in Table 4.4.

Table 4.4: Distribution of Respondent by Education Level

	Frequency	Percent
Diploma	2	2.6
Undergraduate	70	90.9
Master	5	6.5
Total	77	100

Source, Research data (2019)

Table 4.4 shows that 2 out of 77 respondents have attained Diplomas, 70 respondents have attained undergraduate and 5 respondents have attained a master's degree. This represents 2.6%, 90.9% and 6.5% respectively. This infers that the majority (90.9%) of MNOs employees have attained undergraduate.

4.3.4 Distribution of respondents by Duration of Employment

The researcher asked this question to establish the distribution of respondents by duration of employment. The findings are presented in Table 4.5.

Table 4.5: Distribution of respondents by Duration of Employment

	Frequency	Percent
3 to 5 years.	16	20.8
6 to 8 years.	22	28.6
9 to 10.0 year.	13	16.9
More than 10 years.	26	33.8
Total	77	100.0

Source, Research data (2019)

Table 4.5 shows that 16 out of 77 respondents have been employed for between 3 to 5 years, 22 respondents have been employed for 6 to 8 years, 13 respondents have been employed for 9 to 10 years and 26 respondents have been employed for more than 10 years. The results represent 20.8%, 28.6%, 16.9% and 33.8%. The findings infer that the majority (66.2%) of MNOs employees have been working for 10 years and below.

4.3.5 Distribution of Respondents by Organization

The researcher asked this question to establish the distribution of respondents by the organization. The findings are presented in Table 4.6.

Table 4.6: Distribution of Respondent by Organization

	Frequency	Percent
Airtel Kenya	21	27.3
Telkom Kenya	14	18.2
Safaricom PLC	42	54.5
Total	77	100.0

Source, Research data (2019)

Table 4.6 shows that 21 out of 77 respondents are from Airtel Kenya, 14 respondents are from Telkom Kenya and 42 respondents are from Safaricom PLC. This represent 27.3%, 18.2% and 54.5% respectively. This infers that slightly more than half (54.5%) MNOs employees are employed by Safaricom PLC.

4.3.6 Duration of Operation

The researcher asked this question to establish MNOs' duration of operation. The findings are presented in Table 4.7.

Table 4.7: Duration of operation

	Frequency	Percent
10 to 20	70	90.9
More than 20	7	9.1
Total	77	100.0

Source, Research data (2019)

Table 4.7 shows that 70 out of 77 respondents are of the view that MNOs have been in operation for between 10 to 20 years and 7 have been in operation for more than 20 years. This finding corresponds to 90.9% and 9.1% in that order. This infers that the majority (90.9%) of MNO employees concur that MNOs have been in operation for between 10 to 20 years.

4.3.7 Distribution of Respondents by Department

The researcher asked this question to establish the distribution of respondents by the department. The findings are presented in Table 4.8.

Table 4.8: Distribution of respondents by Department

	Frequency	Percent
Transport and IP	9	11.7
Engineering	27	35.1
Network support services	12	15.6
Enterprise	5	6.5
Network operations	5	6.5
Network security	8	10.4
Configuration	4	5.2
Information Technology	7	9.1
Total	77	100

Source, Research data (2019)

Table 4.8 illustrates that 9 out of 77 respondents are in Transport and IP department, 27 are in engineering, 12 are in Network support services and 5 are in the Enterprise Department. The results correspond to 11.7%, 35.1%, 15.6% and 6.5% respectively. The findings also reveal that 5 out of 77 respondents are in Network operations, 8 respondents are in Network security, 4 respondents are in Configuration and 7 respondents are in Information Technology. This represent 6.5%, 10.4%, 5.2% and 9.1% in that order. The finding infers that most (35.1%) of MNOs' employees are in the engineering department.

4.3.8 Number of employees in Department

The researcher asked this question to establish the number of employees in the department. The findings are presented in Table 4.9.

Table 4.9: Number of Employees

	Frequency	Percent
10 to 20	48	62.3
21 to 40	16	20.8
More than 40	13	16.9
Total	77	100.0

Source, Research data (2019)

Table 4.9 illustrates that 48 out of 77 respondents are of the view they are between 10 to 20 employees in the department, 16 agree that they are between 21 to 40 in their department and 13 agree that they are more than 40 employees in their departments. The findings infer that the majority (62.3%) of MNOs employee between 10 to 20 employees per department.

4.3.9 Position Held

The researcher asked this question to establish a position held by respondents. The findings are presented in Table 4.10.

Table 4.10: Position Held

	Frequency	Percent
Network Optimization	15	19.6
Systems Engineer	12	15.6
Core Engineer	5	6.5
Enterprise Service Engineer	5	6.5
Transmission Engineer Support	2	2.6
Radio Access Engineer	5	6.5
Configuration Support Engineer	4	5.2
Cyber Security Administrator	8	10.4
Engineer	7	9.1
Service Desk Support	7	9.1
Manager	7	9.1
Total	77	100.0

Source, Research data (2019)

Table 4.10 illustrates that 15 out of 77 respondents are network optimization engineers, 12 respondents are systems engineers, 5 respondents are core Engineers, 5 respondents are Enterprise Service Engineers and another 5 respondents are Radio Access Engineers. These correspond to 19.6%, 15.6%, 6.5%, 6.5% and 6.5% in that order. Table 4.10 also illustrates that 2 out of 77 respondents are Transmission Support Engineers, 8 are Cyber Security Administrator and 7 are Service Desk Support. This represents 2.6%, 10.4% and 9.1% in that order.

4.3.10 Role Played by Respondents

The researcher asked this question to establish the role played by respondents. The findings are presented in Table 4.11.

Table 4.11: Role Played

	Frequency	Percent
Support Engineers	27	35.1
Systems Engineers	10	13.0
Systems Analysts	8	10.4
Network Operation Engineer	12	15.6
Service Managers	7	9.1
Optimization Engineers	13	16.9
Total	77	100.0

Source, Research data (2019)

Table 4.11 illustrate that 27 out of 77 respondents are Support Engineers, 10 are Systems Engineers and 8 are Systems Analysts. This correspond to 35.1%, 13.0% and 10.4% in that order. Table 4.11 also illustrate that 12 out of 77 respondents are Network Operation Engineer, 7 are Service Managers and 13 are Optimization Engineers. This correspond to 15.6%, 9.1% and 16.9% in that order. The findings infer that most (35.1%) of MNOs employees are support engineers.

4.4 Level of Information Security in Kenya's Mobile Network Operators

The section presents findings on the Level of Information Security in Kenya's Mobile Network Operators. On a 5 to 1 scale, where 5 is greatest extent and 1 is no extent, the researcher required to establish the extent to which MNOs in Kenya secured information. Table 4.12 shows the findings.

Table 4.12: Level of Information Security

	N	Mean	Std. Error	Std. Deviation
Action taken on perpetrators	77	3.53	0.2	1.759
Unauthorized changes compromising the integrity of information	77	3.49	0.171	1.501
Information disappearing from the databases	77	3.84	0.124	1.089
Lack of policies at departmental level	77	3.99	0.143	1.251
Response to attack/attempted attack	77	3.94	0.148	1.301
Exposure of systems to internal or external attack	77	3.79	0.129	1.128
Third Party (Vendors, contractors) security awareness.	77	3.57	0.155	1.361
Information security awareness of the system end users	77	3.91	0.142	1.248
Adequate security policies in place at national level	77	3.75	0.153	1.339
Information leaking to competitors or unintended users.	77	3.23	0.132	1.157
Errors of omission and commission	77	3.45	0.113	0.994
Training staff on security issues at organizational level	77	3.91	0.156	1.369
Overall Mean		3.7		1.29

Source, Research data (2019)

The findings in table 4.12 show that lack of policies at the departmental level, response to attack/attempted attack, Information security awareness of the system end-users and training staff on security issues at the organizational level are rated to a great extent by the respondents. This is represented by mean scores of 3.99, 3.94, 3.91 and 3.91 respectively.

Information disappearing from the databases, exposure of systems to internal or external attack, adequate security policies in place at the national level and third party (Vendors, contractors) security awareness are also rated to a great extent by the majority of respondents. The findings are represented by mean scores of 3.84, 3.79, 3.75 and 3.57 respectively.

Action taken on perpetrators, unauthorized changes compromising the integrity of information and errors of omission and commission was also rated to a great extent. The findings are represented by mean scores of 3.53, 3.49 and 3.45 in that order. It is also evident from table 4.12 that Information leaking to competitors or unintended

users was rated to a moderate extent. This is represented by a mean score of 3.23. The findings infer that MNOs in Kenya has a good level of information system security, as represented by an overall mean of 3.70.

4.5 Challenges of Implementing Information Security of MNOs’ in Kenya

This section presents findings on the Challenges of Implementing Information Security in Kenya’s Mobile Network Operators. On a scale of 5 to 1, where 5 is the greatest extent and 1 is no extent, the researcher sought to establish the extent to which MNOs in Kenya face challenges of implementing information security. Table 4.13 illustrates the findings.

Table 4.13: Challenges of implementing Information Security

	N	Mean	Std. Error	Std. Deviation
Complexities of security attacks.	77	3.9	0.171	1.501
Lack of Support from Top Management.	77	2.96	0.144	1.261
Lack of expertise in managing security issues.	77	3.12	0.15	1.318
Failure to develop security enforcement skills.	77	2.48	0.158	1.382
Budgetary constraints for security infrastructure.	77	3.22	0.171	1.501
Security Policy.	77	2.36	0.112	0.986
Failure to prioritize information security products.	77	2.87	0.153	1.341
Untrustworthy employees.	77	3.39	0.173	1.514
Open discussions of vulnerabilities.	77	2.57	0.163	1.427
Overall Mean		2.99		1.36

Source, Research data (2019)

Table 4.13 shows that the majority of the respondents’ rate complexities of security attacks to a great extent, with a mean score of 3.9. Untrustworthy employees, budgetary constraints for security infrastructure, lack of expertise in managing security issues, support lacking from top management, failure to prioritize information security products and open discussions of vulnerabilities were rated to moderate extent by majority with a mean score of 3.39, 3.22, 3.12, 2.96, 2.87 and 2.57 in that order.

Failure to develop security enforcement skills and Security policies are rated to a less extent. The findings are represented by a mean score of 2.48 and 2.36 in that order.

The findings infer that MNOs in Kenya experience minimum challenges in implementing information systems security. This is represented by an overall mean score of 2.99.

4.6 Mitigation of Information Security challenges in Mobile Network Operators in Kenya

This section presents findings on the Mitigation of Information Security challenges in Kenya’s Mobile Network Operators. On a scale of 5 to 1, where 5 is the greatest extent and 1 is no extent, the researcher sought to establish the extent to which MNOs in Kenya mitigate information security challenges. Table 4.13 shows the illustrates the findings

Table 4.14: Mitigation of Information Security challenges

	N	Mean	Std. Error	Std. Deviation
Strong Authentication of devices	77	4.1	0.144	1.263
Alignment of security strategy to the business specific needs	77	4.45	0.113	0.994
Boosting of Information security Budget	77	4.03	0.129	1.135
Deployment and use of asset management and intrusion detection tools	77	4.38	0.089	0.779
Core Practice deliveries through enhanced training, development, policies enhancements	77	3.74	0.102	0.894
Overall Mean		4.14		1.013

Source, Research data (2019)

Table 4.14 shows that respondents rate all aspects of the mitigation of information security to a great extent. Alignment of security strategy to the business-specific needs mean of 4.45, Deployment and use of asset management and intrusion detection tools mean of 4.38, Strong Authentication of devices mean score of 4.1, Boosting of Information security Budget mean score of 4.03 and Core Practice deliveries through enhanced training, development, policies enhancements mean score of 3.74. The findings infer that MNOs in Kenya mitigate information systems challenges to a great extent, this is represented by a mean score of 4.14.

4.7 Prosperity of Mobile Network Operators in Kenya

This section presents findings on Prosperity. The researcher was concerned with establishing three aspects of prosperity among MNOs in Kenya; meeting the financial target, innovations and net promoter score for the last financial year.

4.7.1 Financial Target

The researcher asked this question to establish if the respondents achieved the set of financial targets during last financial year. The findings are presented in Table 4.15

Table 4.15: Financial Target

	Frequency	Percent
Yes	47	61.0
No	30	39.0
Total	77	100.0

Source, Research data (2019)

Table 4.15 shows that 47 out of 77 respondents are of the view that they achieved financial targets set in the last financial year and 30 did not achieve financial targets set in the last financial year. These findings correspond to 61.0% and 39.0% in that order. The findings infer that the majority (61.0%) of MNOs employees achieved financial targets set in the last financial year.

4.7.2 Innovations

The researcher asked this question to establish if the respondents achieved the introduction of innovation in the last financial year. The findings are presented in Table 4.16

Table 4.16: Innovations

	Frequency	Percent
Yes	54	70.1
No	23	29.9
Total	77	100.0

Source, Research data (2019)

Table 4.16 above shows that 54 out of 77 respondents are of the view that they achieved innovations during last financial year and 23 did not achieve innovations in the last financial year. These findings correspond to 70.1% and 29.9% in that order. The findings infer that the majority (70.1%) of MNOs employees achieved innovations in the last financial year.

4.7.3 Net Promoter Score (NPS)

This section presents findings on the Net Promoter Score in Kenya’s Mobile Network Operators in the last financial year. On a scale of 5 to 1, where 5 is 81% to 100% and 1 is 0% to 20%, the researcher sought to establish the Net Promoter Score of MNOs in Kenya the last financial year. Table 4.17 displays the findings.

Table 4.17: Net Promoter Score

	N	Mean	Std. Error	Std. Deviation
Net promoter score the last financial year	77	3.38	0.111	0.974
Overall Mean		3.38		0.974

Source, Research data (2019)

Table 4.17 shows that the majority of respondents rate the net promoter score for the financial year to range between 41% to 60%. This is represented by a mean score of 3.38.

4.8 Effect of Information Security on Prosperity of Mobile Network Operators in Kenya

This section presents findings on the Effect of Information Security on the Prosperity of Mobile Network Operators in Kenya. The researcher perceived that Information Security affects the Prosperity of Mobile Network Operators in Kenya.

4.8.1 Regression Analysis

This section presents the regression results for the study. First, it presents the model summary, followed by Analysis of Variance findings, and then finally with the findings on Model Coefficients.

4.8.1.1 Model Summary

This section presents findings on the model summary. The results are presented in table 4.18.

Table 4.18: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.778 ^a	.605	.589	.624

a. Predictors: (Constant), MOIS, LOIS, COIS

Source, Research data (2019)

The value of R represents the multiple correlation coefficients that measure the quality of the prediction of the dependent variable. From table 4.18 it is evident that the R = 0.778 for information security shows a strong level of prediction. The R squared which is the coefficient of determination for information security = 0.605 indicating that the model explains 60.5% of the total variance (the adjusted R squares = 0.589) of prosperity in MNOs in Kenya. This means that 60.5% of prosperity in MNOs in Kenya is explained by information security. The remaining 39.5% of the variations in prosperity in MNOs in Kenya is probably explained by other factors and reasons beyond this research.

4.8.1.2 Analysis of Variance

This section presents findings on Analysis of Variance. Table 4.19 presents the findings.

Table 4.19: ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	43.630	3	14.543	37.320	.000 ^b
	Residual	28.448	73	.390		
	Total	72.078	76			

a. Dependent Variable: PRO

b. Predictors: (Constant), MOIS, LOIS, COIS

Source, Research data (2019)

The study was conducted at a 5% significance level. The calculated value is lower than the critical value ($p = 0.000$) which is lower than the significance level of 0.05.

($P < 0.05$). This, therefore, implies that there is a statistical significance. For this reason, we accept the researcher's perception that Information Security affects the Prosperity of Mobile Network Operators in Kenya. .

F value = variance of the group means (Mean Square Between) / Mean of the within group variances (Mean Squared Error). F test indicates the group of variables are jointly significant and the variance between the means is significantly different through testing equality of means. From the findings, ($F = 37.320$), and being a large value indicates statistical significance. This points towards reduced residual variance attributable to the predictor and implies that the variation among group means is more than what would be expected to be seen by chance.

4.8.1.3 Model Coefficients Results

This section presents model coefficients of the study, table 4.20 presents the results.

Table 4.20: Model Coefficients

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.			
	B	Std. Error	Beta					
1	(Constant)	-3.356	.793			-4.234	.000	
	LOIS	.317	.089			.330	3.574	.001
	COIS	.227	.084			.250	2.695	.009
	MOIS	1.179	.156			.685	7.552	.000

a. Dependent Variable: PRO

Source, Research data (2019)

From the regression results in Table 4.20, the regression model equation appears as;

$$PRO = -3.356 + 0.317LOIS + 0.227COIS + 1.179MOIS + \varepsilon$$

The results in table 4.19 imply that Information Security affects the Prosperity of Mobile Network Operators in Kenya. The study was conducted at 5% significance level, the findings show ($p = 0.001 < 0.05$) for Level of Information Security, ($p = 0.009 < 0.05$) for Challenge of Information Security, and ($p = 0.000 < 0.05$) for Mitigation of challenge of Information Security. This implies that there is statistical

significance and for this reason, the test aspects of information security positively affect the prosperity of Mobile Network Operators in Kenya. The study established that Information Security positively affects the Prosperity of Mobile Network Operators in Kenya; Level of Information Security (+0.317), Challenges of Information Security (+0.227), and Mitigation of Information Security (+1.179). The findings imply that a unit increase in prosperity contributes to an increment or increase in information security by a unit of 0.317, 0.227 and 1.179 respectively, indicating the effect Information Security has on Prosperity.

4.9 Discussion of the Findings

The study sought to address four specific objectives. The researcher sought to establish the level of Information Security in Kenya's Mobile Network Operators. The study established that MNOs in Kenya implement information security to a great extent. This is represented by an overall mean score of 3.70 from the findings of the study. Lack of policies at the departmental level, response to attacks/attempted attacks, information security awareness of the system end-users and training staff on security issues at the organizational level are rated to a great extent. However, Information leaking to competitors or unintended users was rated to a moderate extent. The findings are consistent with studies by (Parker, 1988) and (Fenz, 2014) and hence the findings of the literature review interlink with those of the study.

It was also in the interest of the study to determine the Challenges of Implementing Information Security of Kenya's Mobile Network Operators. The study established that MNOs in Kenya rate challenges of implementing Information Security to a moderate extent. This is represented by an overall mean score of 2.99 from the findings of the study. Complexities of security attacks are rated to a great extent by MNOs in Kenya. Failure to develop security enforcement skills and Security policies are rated to a less extent. Ahmad (2017) concur that failure to develop security enforcement skills other than traditional information technology has been viewed as a major challenge. Snekenes (2018) is of the view that challenges are regarded as significant issues. Broadly, the challenges can be grouped into people and access control, with people inadvertently doing things they should do or not, or solely not having proper access control on a system.

The study further sought to find out the extent of Mitigation of Information Security challenges in Mobile Network Operators in Kenya. The findings of this research expose that MNOs to a great extent mitigate challenges of Information Security. This is reflected by an overall mean score of 4.14. Respondents rate all aspects of mitigation of Information Security challenges to a great extent, however, it should be noted that Core Practice deliveries through enhanced training, development, policies enhancements are rated the lowest. This is represented by a mean score of 3.74. Ismail (2015) reports that as a result of their respective vast networks and potential risks and challenges, mobile network operators have armed themselves by putting in place structures and strategies to mitigate the attacks. Management of information risks requires adeptness to combat and neutralize the attacks (Geer, 2001).

Finally, it was also the concern of the study to investigate the effect of Information Security on the Prosperity of MNOs' in Kenya. The researcher perceived that Information Security affects the prosperity of MNOs' .The study was conducted at 0.05 confidence interval. The findings established ($R = 0.778$, & $R^2 = 0.605$), while (Adjusted $R^2 = 0.589$). The findings infer a strong level of prediction that Information Security affects the Prosperity of Mobile Network Operators in Kenya. This means that 60.5% of Prosperity in MNOs in Kenya is explained by Information Security. 39.5% of the variations in Prosperity in MNOs in Kenya is explained by factors and reasons beyond the research

Analysis of variance results show ($p = 0.000$) which is lower than the significance level of 0.05. This indicates statistical significance, implying that Information Security affects the Prosperity of Mobile Network Operators in Kenya. The findings of the study further expose that ($p = 0.001 < 0.05$) for level of information security, ($p = 0.009 < 0.05$) for Challenges of Information Security and ($p = 0.000 < 0.05$) for Mitigation of challenges of Information Security.

The Level of Information Security, Challenges of Information Security and Mitigation of Challenges of Information Security all have a positive effect on the Prosperity of MNOs in Kenya. The Beta scores for the level of information security (0.317), the challenge of information security (0.227) and mitigation of information security (1.179). This infers that a unit increase in prosperity contributes to an increment or

increase in information security by a unit of 0.083, 0.221 and 0.067 respectively. These findings are consistent with (Blakey, 2001), (Hunter & Kelly 2005), and (Tallerro & Gaudette 2010)

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter presents a summary of the study's key findings, the conclusion made from the findings, recommendations as per the findings and recommendations for additional research.

5.2 Summary of the Findings

This study generally focused on establishing the overall effect of information Security on the prosperity of MNOs' in Kenya. Foremost it sought to establish the level of information security in Mobile network operators in Kenya. The findings established to a great extent that MNOs' in Kenya do implement Information Security indicated by an overall mean score of 3.70. On policy issues at the departmental functional level, response to attacks/attempted attacks, information security awareness of the system end-users and training staff on security issues at the organizational level the study rated that to a great extent. On the issue of Information leaking to competitors or unintended users the study rated that to a moderate extent.

Looking at the study's interest to determine the challenges of implementing Information Security of MNOs' in Kenya, the study determined that MNOs' to a moderate extent do face challenges while Implementing Information security however worth noting was the great extent rating on the issue of complexities of Security attacks within the operators. Other issues were rated to a less extent indicating that even though MNOs' in Kenya face challenges, the established score regards the challenges as significant which prompted for further grouping into people and access control.

On the extent of Mitigation of Information Security challenges in MNOs' in Kenya, the findings exposed that to a great extent MNOs' mitigate challenges of Information Security reflected by an overall mean score of 4.14. All aspects of mitigation of Information Security challenges were rated to a great extent whereas most aspects were rated highly, the issue of Core Practice deliveries through enhanced training, development, policies enhancements was rated the lowest thus presenting a new area

for future or further research. The study finally established that Information Security does have an effect on Prosperity of MNOs' in Kenya, indicated by the strong level of prediction. From the study, the Level of Information Security, Challenges of Information Security and Mitigation of Challenges of Information Security all were found to have a positive effect on the Prosperity of MNOs in Kenya.

5.3 Conclusion

The research was concerned with establishing the level of Information Security in Kenya's Mobile Network Operators. The study concludes that there is a great level of Information Security implementation among MNOs in Kenya. Despite the success in this front, MNOs lack information security policies at the departmental level. In the interest of this study to determine the challenges of implementing Information Security by Kenya's Mobile Network Operators, the study concludes that MNOs face limited implementation challenges, however, the complexities of security attacks still present a major challenge experienced by MNOs in Kenya. The study sought to find out the extent of mitigation of Information Security challenges in Mobile Network Operators in Kenya. The study concludes that MNOs in Kenya mitigate information Security challenges to a great extent. However, the adoption of core practice deliveries through enhanced training, development, policies enhancements is not highly adopted by MNOs in Kenya. Finally, the study investigated the effect of Information Security on the Prosperity of Mobile Network Operators in Kenya and concluded that Information Security positively affects the Prosperity of Mobile Network Operators in Kenya.

5.4 Recommendations

The study established that Information Security positively affects the Prosperity of Mobile Network Operators in Kenya. Despite this MNOs lack information security policies at the departmental level and there are complexities of security attacks. Moreover, the adoption of core Practice deliveries through enhanced training, development, policies enhancements is not highly adopted by MNOs in Kenya. Based on this, the study recommends that;

1. Mobile Network Operators in Kenya should adopt a bottom-up approach to Information system security. This will ensure departmental inclusivity as

security of information system starts with users who are attached to different departments.

2. Mobile Network Operators in Kenya have to enhance information security policies to address core practice deliveries, this can be achieved through training and development of users.
3. To address the complexities of security attacks, MNOs' need to invest more in the detective Information Security system to offer futuristic solutions to complex problems.

5.5 Limitation of the Study

The conclusions of the research were primarily applicable and restricted to the Mobile network operators in the industry but could apply to other related technological oriented industries and this would require further exploration

5.6 Suggestion for Future Research

Future studies can focus on the area of Information security training and compliance for none IT users, and also explore the effective ways of handling presented complexities of information security attacks in the industry.

REFERENCES

- Alexander, S., (1999 September). *Speech Recognition* Computer world top-flight technology.
- Anthes, G., (1998 October). *Biometrics*. Computerworld/when Five 9s aren't enough.
- Applegate, L., & Robert, D. (2003). Corporate information system.
- Andrews, D., (2004). Information systems of National security. *Security Committee*. National Information Systems Security (INFOSEC).
- Alfawaz, S., May, L., & Mohanak, K. (2008). Security in developing countries:
- Almeida, F. L. (2009). *Creation of Value with Open Source Software in the Telecom Field*
- Ataya, S., (2006). *Information protection IS Governance*.
- Barney, J., (1991). *Journal of Management*.
- Boston, B., & Fraser, P. (1991). Ethical issues in an information system.
- Boutin, P., *Burn baby burn*. (December 2002).
- Barney, J., (2015). *International Business Strategy: Theory and Practice*.
- Birudavolu, S., & Nag, B. (2011, November). *A Study of Open Innovation in Telecommunication services: A Review of Literature & Trends*. Indian Institute of Foreign Trade.
- Bryan, L., & Wilhelm, R. (1999). *Race for the world: Strategies to build a great Global Firm*. Boston: Harvard Business school press.
- Cooper, D.R., & Schindler, P. (2003). *Business Research Methods*. (8th Ed.). Boston: 15 McGraw-Hill Irwin.
- Deckmyn, D., (2015). More Managers monitor E-MAIL. *Ethical issues in an information system*.

Diego , K., Fernando , M. R., Paulo, V., Rothenberg, E. C., Azodolmolky, S., & Uhlig, S. (2014). *Software Define Networking: A Comprehensive Survey*.

Dhillon, G., &Torkzadeh, G. (2006). *Value-focused Assessment of Information Systems Security in Organizations*, Information Systems Journal16 (3), 293-314.

Dunlop, C., &Rob, K. (1991). Computerization and controversies: *Value conflicts and social choices*. A Diego: Academic press.

Dunlop, T.,(September-October 1996).Values in Tension: *Ethics away from Home*. Harvard Business Review.

Friedrich, R., Bartlett, C., Gröne, F., & Mialaret, N. (2013). *Enabling the OTT revolution: How telecom operators can stake their claim*. Booz & Company.

Grabosky, P., Smith, R., & Dempsey, G. (2001). *Electronic Theft: Unlawful Acquisition in Cyberspace*. Cambridge University Press.

Johnson, D., (1997).*Ethics online*. Communication of the ACM.

Kalakota, R., & Marcia, R.(2002).E-business roadmap for success.

Kovacheva, T., (2010). Information Technologies for Strategic Management. *Computing and information security in systems*.

Kankanhallia, A., Teo, H., Tan, B., & Wei, K. (2003). Study of Information Systems Security Effectiveness, International Journal of Information Management.

Lenardon, J., (2006). *Identity theft toolkit; how to recover from and avoid identity theft*, International self. Counsel press.

Legrisa, P., Ingham, J., & Collette, P. (2001). People using Information Technology. A critical review of the technology acceptance model. *Information & Management*.

Milner, G., (2004). Phishing scams increase 180% in April aloneBankersonline.com

Micheal, V., (2001). *A place to space: Migrating to E-business models*. Harvard Business School Press.

Omwansa, T., (2009). *M-PESA: Progress and Prospects innovations / Mobile World*.

Radicliff, D., (January 14, 2002). *Cyber sleuthing Solves the case*.

APPENDICES

APPENDIX 1: QUESTIONNAIRE

SECTION A: DEMOGRAPHICS

1. Name of your Organization

- Airtel Kenya
- Telkom Kenya
- Safaricom PLC

2. What is your Age cluster?

- >23 Years 24 - 27years
- 28 - 31 years 32 -36 years
- 37 - 41 years Over 41years

3. Highest attained educational level: Certificate Diploma University Masters PhD

4. What is your Gender?

- Female
- Male

5. Length of period your organization been in operation

.....
.....
.....
.....
.....

6. Length of period you have you worked in the organization.

- Below 6 months 1- 2 years
- 3 - 5 years 6 - 8 years
- 9 -10 years Above 11 years

7. Identify your departmental function in the Organization

- Transport and IP
- Engineering
- Network support services
- Enterprise
- Network Security
- Configuration
- Network Operations
- Information Technology
- Product Development and Innovation

Other, please specify

.....

.....

.....

.....

.....

8. Current Position held

.....

.....

.....

.....

.....

9. How many employees does your Section have?

- > 20
- 11 - 20
- 21- 40
- > 41

10. Which of the following best represents your role in the organization?

- Support Engineer
- System Engineer
- Security Engineer

- () System Analyst
- () Network Operation Engineer
- () Service Management

Other, please specify

.....

.....

.....

.....

.....

SECTION B: LEVEL OF INFORMATION SECURITY

Below are several factors that may indicate the level of information risk exposure in organizations.

To what extent has the operator secured Information?

Using a Likert scale of 1-5 where, 1=no extent, 2=less extent, 3= moderate extent, 4=great extent and 5=greatest extent

Key Indicator	<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>
The action was taken on perpetrators					
Unauthorized changes compromising the integrity of the information					
Information disappearing from the databases					
Lack of policies at the departmental level					
Response to attack/attempted attack					
Exposure of systems to internal or external attack					
Third-Party (Vendors, contractors) security awareness.					
Information security awareness of the system end-users					
Adequate security policies in place at the national level					
Information leaking to competitors or unintended users.					
Errors of omission and commission					
Training staff on security issues at the organizational level					
Any other specify below					

SECTION C: CHALLENGES OF INFORMATION SECURITY

Below are some of the factors contributing to information security challenges

To what extent is the following a challenge to information Security?

Using a Likert scale of 1-5 where, 1=no extent, 2=less extent, 3= moderate extent, 4=great extent and 5=greatest extent

Key Indicator	1	2	3	4	5
Complexities of security attacks					
Support from Top Management					
Lack of expertise in managing security issues					
Failure to develop security enforcement skills					
Budgetary constraints for security infrastructure					
Security Policy					
Failure to prioritize information security products					
Untrustworthy employees					
Open discussions of Vulnerabilities (Enlightening users of the problem)					
Any other specify below					

SECTION D: MITIGATION OF CHALLENGES OF INFORMATION SECURITY

How do you rate factors adopted by your organization to mitigate information security challenges.

To what extent is the following a mitigation to challenges of information Security?

Using a Likert scale of 1-5 where, 1=no extent, 2=less extent, 3= moderate extent, 4=great extent and 5=greatest extent

Key Indicator	1	2	3	4	5
Strong Authentication of devices					
Alignment of security strategy to the business specific needs					
Boosting of Information security Budget					
Deployment and use of asset management and intrusion detection tools					
Core Practice deliveries through enhanced training, development, policies enhancements					
Any other specify below					

SECTION E: INFORMATION SECURITY AND PROSPERITY

The following are the questions for Information Security and Prosperity

INFORMATION SECURITY

1. Does your Organization own a document for Business continuity and Disaster Recovery?

YES	<input type="checkbox"/>
NO	<input type="checkbox"/>
NOT SURE	<input type="checkbox"/>

How often is the policy reviewed?

.....

.....

.....

.....

.....

2. How would you rate your overall experience with the quality of the information in your organization being true or correct in the last financial year?

TRUE	<input type="checkbox"/>
VERY TRUE	<input type="checkbox"/>
NOT TRUE	<input type="checkbox"/>

3. Do all individual employees with access to the data and network sign off a confidentiality and non-disclosure agreement within a predefined performance period?

YES

NO

NOT SURE

If so, how are these agreements enforced?

.....
.....
.....
.....
.....

4. Does your organization have a policy that addresses information classification?

YES

NO

If so describe its effectiveness in the preservation of your Organization's information confidentiality

.....
.....
.....
.....
.....

SECTION F: PROSPERITY

1 Have you met your annual financial targets? YES

NO

2. Did your department come up with any innovations in the last financial year?

YES

NO

3. Rate your Net promoter score in the last financial year.

*Using a Likert scale of 1-5 where, 1=0% to 20%, 2=21% to 40%, 3= 41% to 60%
4=61% to 80% and 5=81% to 100%*

	0%- 20%	21%- 40%	41%- 60%	61%- 80%	81%- 100%
Mobile Network Operator					
SAFARICOM PLC					
AIRTEL KENYA					
TELKOM KENYA LTD					