CORPORATE SECURITY MANAGEMENT STRATEGIES AND PROFITABILITY OF THE TELECOMMUNICATIONS FIRMS IN KENYA.

KAIREMIA DENIS KIMATHI

D53/OL/CTY/29118/2014

A RESEARCH PROJECT SUBMITTED TO THE SCHOOL OF BUSINESS IN PARTIAL FULFILMENT FOR THE AWARD OF DEGREE IN MASTER OF BUSINESS ADMINISTRATION (STRATEGIC MANAGEMENT OPTION) OF KENYATTA UNIVERSITY.

APRIL, 2019

DECLARATION

I do declare that this research project is my original work and has not been presented for a degree or any other award in any other university. No part of this research project should be reproduced without the authority of the author or/and Kenyatta University.

Sign …… Date ……

KAIREMIA D.K D53/OL/CTY/29118/2014

Department of Business Administration

This research project has been submitted for examination purposes with my approval as the university supervisor.

Sign …… Date ……

DR. MARY RAGUI, PhD

Department of Business Administration

School of Business

Kenyatta University

DEDICATION

I want to dedicate this research project to my family who supported me through the whole time. I also want to dedicate it to my supervisor for her guidance and support.

ACKNOWLEDGEMENT

I acknowledge the support and guidance of my supervisor Dr Mary Ragui in the long journey towards the development of this research project.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

ALE	Annualized Loss Expectancy
ARO	Annual Rate of Occurrence
CEO	Chief Executive Officer
CSO	Chief Security Officer
EAS	Emergency Alert System
EFCS	External Function of Corporate Security
IFCS	Internal Function of Corporate Security
ROI	Return on Investment
SLE	Single Loss Expectancy
SMS	Short Message Services
TelCo	Telecommunications Corporation
VOIP	Voice Over Internet Protocol

OPERATIONAL DEFINITION OF TERMS

Contract security – Also referred to as outsourced security. It is a corporate security management strategy whereby a corporation hires a private security provider to provide security services for the given corporation.

Corporate security – This is the employment of security personnel or equipment directly or indirectly to safeguard assets, personnel and even profitability as well as risk management.

Corporate security management strategies – These are security management strategies adopted by a corporation. They are defined by the relationship between the corporation and the security personnel.

Hybrid corporate security management strategy – This is a corporate security management strategy whereby a corporation employs a mix of proprietary security and contract security personnel. In this strategy the corporation does not use either proprietary or contract security but uses all of them in varying proportions.

Outsourced security management strategy – Also known as contract security strategy, it is the practice in corporate security whereby a corporation contracts a private security firm to provide security services to the given corporation.

Profitability–This is the difference between expenditure and revenue. It is the metric used to determine the scope of a company's profit in relation to the size of the business. It is a measurement of efficiency in getting returns from an investment.

Proprietary corporate security management strategy – This is the practice of corporate security where a corporation entirely uses security personnel hired directly by the corporation and managed by the human resource of that corporation like any other employee. All the security equipment in this strategy is used exclusively by that corporation.

ABSTRACT

Corporate security has evolved immensely over the past few decades, from a simple egress control task to a corporate management function with a sizable budget and sometimes a seat in the board with the task of ensuring business continuity. The broadened role of corporate security has meant more stakes on its success and therefore more scrutiny and funding. This study sought to examine how the employment of the various security management strategies affects a given organization's profitability by considering both direct and indirect costs. This study explored four theories that define the relationship between corporate security management strategies and profitability. The theories are; mitigation value theory, internal function of corporate security theory, external function of corporate security and the revenue potential theory. Firms in the Kenya Telecommunications industry cannot ignore the value of corporate security, but in this regime of cut-throat competition and the corporations desire to keep their bottom-line healthy, three different corporate security management strategies have emerged namely; proprietary corporate security management strategy whose relationship with profitability was 0.195 at .0239 confidence level, outsourced corporate security management strategy whose relationship with profitability was 0.308 at .0224 confidence level and the hybrid corporate security management strategy whose relationship with profitability was 0.335 at .0217 confidence level. The study targeted Corporate security practitioners in the Kenyan telecommunications industry as the target population. Census sampling was used and the sample size was 67. This study used a questionnaire and the data collected analyzed by the use of SPSS and the ANOVA test. The study found that proprietary security strategy is reliable, the security workers are loyal and trustworthy. However, the emoluments, training costs and recruitment costs are high. The study established savings on training, equipment and efficiency is enhanced but trust and reliability are sub-optimal. The study established that security providers under all the security management strategies are sourced from the same labor market. The study finally established that with hybrid security system; efficiency is enhanced, emoluments are low, contract costs are low but trust is not optimal. The study also found out that there are more security related incidences reported under both outsourced and hybrid management strategies and outsourced security providers do not underwrite any security incidences that lead to lose in premises they are contracted to secure. The study recommended for the top management of the telecommunication companies to evaluate their business well based on the different benefits as well as drawbacks with the different options for strategic security. They should proprietary for reliability and trust and choose to suffer higher emoluments costs that has effects on profitability or go for the other forms and have low contract costs but loose trust and reliability. The study also recommends that contracted security providers should underwrite a proportion of loses suffered under their care to increase reliability.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The telecommunications industry in Kenya has for a number of years now epitomized the advancement of technology in the country while forming the country's economic backbone due to mobile money transfers and ease of communication accounting for a sizeable percentage of the GDP. Its contribution to GDP and its representation of the western technology has made the industry a target for terrorists while its abnormal profits has led to a lot of competition in the industry. This has posed a security issue that needs to be managed under limited budgetary wriggle-room as corporations in the industry struggle to remain within competitive running costs.

This study examines the practice of corporate security and how various management strategies affect a corporation's profitability. In this study a corporation is defined as any organization that takes on employees to achieve a definite common goal either as a commercial entity or a government instrument (Georg, 2004). While this definition encompasses a myriad of different organizations all of them have a similar bottom-line; they must operate in a financially responsible way, which means cost management and asset security.

Corporate security is the safeguarding of the forte, personnel and even profitability of an organization against theft, fire, fraud, criminal damages and acts of terrorism (McGee, 2006). In this definition of corporate security, it is evident that it encompasses both physical and the non-physical aspects. The purview is also broadened to include the profitability of the organization.

Nalla, (2002) also defined security as a corporation's management of risk to their people, property, information and liability. That being the definition of corporate security then corporate security management strategies is the different practices employed by corporations to manage risk to their employees, property, information and the going concern of their corporations. The use of corporate security enables the organization to prohibit conduct it presumes as detrimental to its profit build-up. This conduct however, may not necessarily be deemed as illegal.

Business organizations are able to modulate the minutiae of conduct happening in their private spaces and neglect traditional due process rights (Calder, 2007). Accordingly, corporations are able to deal with traditional and new security challenges promptly. Addressing security challenges promptly enables organizations to mitigate what would otherwise have been costly threats of actual security challenges.

The decision on whether to use contract security or proprietary security to manage a corporation's security does not lie solely on comparative costs. The hidden costs and risks also need to be evaluated and considered. A professional in-house security that is well managed and tailored in the organizations culture has value beyond the apparent cost saving (Sennwald, 2003).

The Kenya telecommunications industry is uniquely challenged in terms of corporate security management strategies for many reasons including the need to maximize return on investment by ensuring value for money, the susceptibility of the telecommunications infrastructure to sabotage, the cost of security breaches in the industry and the need to protect business secrets (Adum, 2006).

Every corporation's management understands that security is an inevitable expense. Security management is not an eccentric but essential back-lot function. It is instead, a crucial business function that is paramount to any organizations continued viability (Dalton, 2003). Corporate

security is essential regardless of the associated costs. To continue to be able to assure business continuity, security must be treated as a vital corporate function and resourced accordingly.

While this shows that corporations have really no choice in whether to have security or not, each and every corporation must operate in a financially responsible way (Challinger, 2010). Considering these facts therefore it becomes important that a manager makes an informed choice of the corporate security management strategy that maximizes contribution. The balance between minimizing costs and ensuring security for the organization must be delicately found and toed.

1.1.1 Profitability

Profitability is the ratio between expenditure and revenue in a profit-making organization. Every profit-making organization must find the most prudent management strategy that minimizes costs while maximizing revenues. Profitability is a factor of cost and revenue and therefore the relationship between corporate security management strategies and profitability can be evaluated either by cost and revenue individually or both. The broadening purview of security threat is requiring security divisions to become more affiliated with the core objective by moving ‘security as a cost’ to ‘generating utility from security’ (ASIS International, 2010).

The cost implications of corporate security go beyond the outlay in emoluments for proprietary security and the costs of contract in outsourced security and the security equipment purchase (Lanfranchi, 2000). In situations where practices or activities of corporate security are viewed as a nuisance, a cost is incurred though indirect and this affects the profitability of the given corporation. In a telecommunications industry for example, encryption in communication increases the end to end latency which might be a nuisance to some customers who in turn reduce their calling or shift to other networks all together.

According to McGee, (2006) the modern state of corporate security, its professional standing and the potential for further professionalization of the occupation. This, while important in the practice of corporate security, it is important to note that further professionalization of the occupation costs money. Without the evaluation of how every corporate security management strategy affects profitability, it is hard for the corporation to determine whether further investment in the professionalization of the occupation will give value for money.

How the professionalization of the occupation is carried also will vary and the costs will depend on strategy that a corporation adopts to manage its security. For example, if the professional institutions are owned by the private security providers then the professional fees would be cheaper for contracted security while proprietary security would be charged prohibitive fees to encourage security contracting. It could also lead to low professional standards on the part of the contracted security as they seek to cut costs (Moresh, 2002).

Corporations need to remain profitable and by minimizing costs and at the same time ensuring that their profitability is sustainable brings about the challenge of trading off cost and benefits of any given department or venture in that organization (Halibozek, 2003). That considered, corporation's management will always seek to strike the right balance between the need for sustainability and the implications of the investment on sustainability of the company's profitability in the short and medium term. In order to make the best choices with regard to corporate security, management needs empirical evidence of how the various strategies the corporation might adopt to manage its security affects the profitability of the organization. Organizational security affects the profitability of the given Corporation in two ways; cost and benefits. The management must therefore adopt a strategy that assures the corporation the biggest positive spread.

In order to provide the required information, this study identified both the costs and benefits of the various strategies that may be adopted and cost them so as to determine their value to the corporation. According to Holden, (2000) currently these decisions are made by the management of the various corporations based on assumptions that have not been empirically proven; we fashion management and financial decisions grounded on an inordinate number of unproven conjecture.

It is assumed that corporate security as a profession is both uncodified and substantially unproven. It's assumed that security officers proffer some deterrent utility and that modern cutting-edge technologies are potent in arresting loss of resources and life (Dalton, 2003). The decisions about the corporate security management strategies may also not solely depend on the availability or the lack thereof. Politics being what they are, it's too facile for resolutions (about security) to be imprudent when intramural politics are allowed to infiltrate the fray.

With loss prevention delineated to a manager, that licenses him to set the tone, the direction, about what efficacious diminution prevention is (Lee, 2002). To alleviate these assumptions this study identified the various facts that relate to the practice of corporate security and how that affects profitability. Those aspects of the business that are directly or indirectly affected by the practice of corporate security must were assessed and quantified.

Canton, (2003) also identifies the benefits of each of the corporate security management strategies as well as the costs that are related to the strategies uniquely. However, he also fails to relate the benefits and costs directly to the profitability of the corporations under study. Though the costs and revenue directly or indirectly attributed to corporate security are documented, how they relate to the profitability of the given organization is not well articulated.

1.1.2 Corporate Security Management Strategies

Different scholars and management gurus have identified differing number of corporate security management strategies. There are two main corporate security management strategies, which are; proprietary corporate security and contract security (Prentice, 2005). Accordingly, a corporation may choose to employ security practitioners as it employs other employees or it may choose to contract a private security company to provide corporate security services to that corporation.

There are three major corporate security management strategies. A corporation may choose any of these strategies to manage its security; proprietary security, contract security or hybrid solutions (Bradford, 2009). The strategy that a corporation chooses to manage its security will depend on a number of things that include; relatable costs, perceived benefits, organizational size, actual and perceived threats, organizational culture and management policy.

The strategy chosen by the management may also be determined by the management's attitude towards security. Pre-eminent security keeps the entire corporations' assets secure – and therein lays a paradox. The triumph of organizational security is appraised on the imprevalence of activities which would have undesired sequel on the corporation if they occurred. Put in a different way, a decidedly efficacious security manager may become the casualty of their own success (Challinger, 2010). The absence of security threats or incidences which could have resulted from good security management may be perceived as indicators that the security costs can be avoided.

Proprietary security also known as in-house security is a corporate security management strategy that is characterized by the direct recruitment of its corporate security staff by the Human Resource function of that organization. If the security department in an organization is made up of the corporation's employees then that is considered as an in-house corporate security management

strategy. Corporations that opt for this security management strategy are inspired by reasons that include; ensuring the right level of training is achieved by the staff, ensure loyalty, the organizational ethics can also be enforced on proprietary security (Bradford, (2009).

Security officers directly employed by a corporation are more reliable, have direct relationship with the corporate management and the degree of training is up to the standard that the corporation chooses (Holden, 2014). This corporate security management strategy has its challenges also, that might include diversion of key resources and manpower into the recruitment of security a non-core function of the corporation and this may have negative effects on the corporations bottom-line.

According to Holden the cost of this strategy is also higher than other strategies; a full time employee will normally include additional costs like vacation, taxes, benefits, overtime, annual raises and holiday pay (Holden, 2014). This study sought to monetize all the advantages and disadvantages of proprietary security so as to determine the net contribution of the adoption of this corporate security management strategy on the corporation's bottom-line.

Contract security which is also known as outsourced security is the security management strategy that involves a corporation's management outsourcing its security to a private corporate security provider. Many diverse reasons are cited by corporations for their choice of this corporate security management strategy including cost and time. The reason most cited for outsourcing security is the cost implication, however, focusing on the theme of cost while being oblivious to effectiveness is myopic (Challinger, 2010).

Further Dalton dispenses of the myth behind the push for outsourcing security staff to cost save. He says, they come from the same labor pool as the internally employed staff (Dalton, 2003). This

in essence, therefore, means that regardless of whether the security personnel are recruited directly or through a contracted third party the cost will have no significant difference given both corporations recruit from the same labor pool. Outsourcing corporate security however improves risk spread in a corporation.

Hybrid corporate security management strategy is mix between proprietary and outsourced security regardless of the proportions of each. According to Bradford (2009) proprietary security has its benefits and its disadvantages over both proprietary and outsourced security, consequently some corporations have sought to engage a strategy that seeks to maximize on the benefits of each while cutting down on the disadvantages by employing a mix of both. The hybrid security management strategy sometimes involves the outsourcing of the basic protective security services while the more complicated issues including management are handled by in-house security.

To evaluate the effect of the various corporate security management strategies on a corporation's profitability, there is need to identify the metrics on which the costs and benefits each of the employment of each of the strategies provides. Organizations have long sought to catalogue metrics and measures that may be applied to reliably indicate the value corporate security brings to a corporation while focusing on the annual earnings, departmental budgets and incident statistics (Campbell, 2011).

Campbell further identified the CSO dashboard as one key metric in measuring the effectiveness or the lack of it of a given security strategy. The contents of the dashboard would vary with every organization depending on the industry, relations with third parties and the general operational environment. In the case of the Kenyan telecommunication industry a CSO dashboard would be expected to have among others infrastructure in NEP and North Coast, security audits, proportion

of employees with background issues, cyber intrusion, year to year investigative findings, security cost per unit of revenue and the variance in security patches (Campbell, 2011).

According to Dalton (2003) "security management is not a backlot function but is instead a function that is critical to a business continued survival. Therefore, corporate security is very key to the firms' long-term viability as may be evidenced by the statistics from the Communications Authority on security threats reported." In the financial year 2014/2015 criminal use of services and facilities was ranked third in the customer complaints against telecommunications industry players with 21 complaints, which however was a decline from the 43 complaints in the previous year behind unauthorized charges/subscriptions and billing in first and second positions respectively. These numbers would also rise significantly when security is looked at in the broader perspective as there would be additional incidents like the 8 complaints recorded in the same years for breach of confidentiality/privacy that completely falls within the purview of corporate security responsibility. Customers who feel being in a given network breaches their confidentiality and privacy because of weak information control systems or rogue employees may most of the time shift to other networks that are more privacy concerns sensitive.

1.1.3 The Telecommunications Industry in Kenya

The telecommunications industry is a corporate sector that deals with communications for the public in commercial scale and for commercial purposes (Edelson, 2000). Due to the advent in technology over the past few decades, the telecommunications industry has grown tremendously as the cost of infrastructure per individual customer has gone down and so has the cost of termination gadgets making them more accessible to the general public.

The returns that are associated with the telecommunications industry has led to very high competition in the industry. While this study focuses on the entire telecommunication industry in Kenya, there are players in this industry who exist in the fridges of the industry. This study focused on those telecommunications firms who have the infrastructure in at least every county in the country and whose core business is telecommunications. There are three such firms in Kenya; Safaricom, Airtel and Orange (CAK, 2015).

This study focused on the three biggest corporations in the industry as they have countrywide reach in terms of services and infrastructure. Equitel a telecommunication service provider also in Kenya is an offshoot of the country's largest bank by customer numbers has no infrastructure throughout the country and its services depend on another service provider's infrastructure (Buddie, 2015). Corporations like Kenya Data Networks do not qualify as it only deals with one aspect of telecommunications which is internet provision and its subscriber base is less than a million.

Corporate security is largely mainly grounded on presuppositions. Management and financial resolutions are made founded on an inordinate number of unproven conjecture. It is a vocation that is uncodified and substantially unproven. It is assumed that security provides some dissuasive value (Dalton, 2003). This happens due to the lack of empirical data to support informed security management decisions.

The communications authority of Kenya also in their annual report for the year 2015 listed on three telecommunications service providers as having mobile cellular systems.

According to the communications authority of Kenya the telecommunications industry in Kenya has had its market shared as in the table below between the key players in the industry.

Service provider	Number of subscribers	percentage
Safaricom	23.3M	67.1%
Airtel	7M	20.2%
Orange	3.7M	10.8%

Figure 1.1: The Kenya Telecommunications Industry Market Share

Source: Communications Authority of Kenya

1.2 Statement of the Problem

The telecommunications sector in Kenya is one of the most profitable in the country and in the region, with Safaricom being the most profitable company in the region. Good returns in business brings with them fierce competition as may be evidenced by the entry of players like Equitel. The cutthroat competition in the industry can be exemplified by the statistics from the communications authority of Kenya where in the first quarter of 2015/2016 Safaricom lost 1.7% market share, Airtel lost 0.3% and Orange gained 1.0% in the same period (CAK, 2016). This, in essence therefore means that to remain competitive and profitable, the firms must be mindful of their customer perceptions and the costs.

According to the Communications Authority of Kenya complaints statistics from the regulatory year 2014/15. The complaints made to the regulatory body with regard to crime associated with the use of the telecommunication infrastructure laid by the leading Telcos in the country in the cyberspace consisted of Fraud at 29%, both Denial of Service, Phishing and Spamming at 22%, online abuse at 19% and SQL Injection at 8% CAK (2015). These are all reported crimes supposedly committed on platforms provided by the telecommunication firms.

In an industry where there is cut throat competition, organizations must maximize their returns while minimizing their expenditure and ensuring business continuity in the long-run. To manage this, organizations must make informed decisions on the corporate security management strategy to adopt so that they maximize revenue, minimize cost and at the same time ensure business continuity (Lee, 2002).

The telecommunications industry is uniquely positioned at a place where insecurity costs are exponential be they direct like vandalized equipment due to their cost and indirect costs that may result in system downtimes should the system lack enough redundancy to support the customers. The cost of the equipment makes them attractive to thieves and the significance of the industry to the economy makes them attractive terror targets.

The competitiveness in the industry has led to price wars reducing profit margins. This has resulted in cost management measures to maintain profitability. Bearing this in mind, corporations in the industry must endeavor to employ the most efficient strategies leading to better value for money.

Faced by the two problems of reduced profit margins necessitating cost management measures and the increased security vulnerability. The corporations must establish security management strategies that addresses their security concerns while at the same time remaining within their cost margins to remain cost competitive in the industry flooding with competition.

This study sought to provide empirical data to buttress the choice of corporate security strategy by firms in the Kenya telecommunications industry based on their effect on the profitability of the given organization.

1.3 Objectives of the Study

1.3.1 General Objective

To examine the correlation between corporate security management strategies and profitability in the telecommunications industry in Kenya

1.3.2 Specific Objectives

This study sought to investigate the relationship between corporate security management strategies and profitability in the telecommunications industry in Kenya. To do that, the following specific objectives were pursued.

(i) To examine the consequence of using proprietary corporate security management strategy on profitability in the telecommunications industry in Kenya.

(ii) To determine the implications of outsourcing corporate management security strategy on profitability in the telecommunications industry in Kenya.

(iii) To establish the implications of hybrid corporate security management strategy on profitability in the telecommunications industry in Kenya.

1.4 Research Hypotheses

Hypothesis are single provisional postulates assumed for use in formulating theory or designing experiments purposed to give a diametric experimental assessment when practicable. Relational hypothesis is describing the relationship between corporate security management strategies and profitability. Relational hypothesis aims to determine if a relationship exists between a set of variable values (Williams, 2003). Relational hypothesis may have no direction at all. The technique is adequate in purpose and seeks to confirm or disapprove;

H_{01}. There exists no relationship between proprietary corporate security management strategy and profitability in the telecommunications industry in Kenya.

H_{02}. There exists no relationship between outsourced corporate security management strategy and profitability in the telecommunications industry in Kenya.

H_{03}. There exists no relationship between hybrid corporate security management strategy and profitability in the telecommunications industry in Kenya.

1.5 Significance of the Study

This study attempted to evaluate how the organizational security management strategies affect the profitability of corporations in the telecommunications industry in Kenya. Corporate security has become a very key function in modern day corporations as security challenges intensify due to the polarization of the world, technological advancement and cutthroat competition among corporations in the same industry. With corporate security continually viewed as a 'necessary evil' where corporations have no choice Halibozek (2003) this study comes in handy to provide some much-needed information to corporations' managements'. The result of this study informs the choices made by CEOs and Boards on the corporate security management strategies.

Improved security management efficiency as a result of an informed choice of the approach as guided by the findings of this study will lead to improved security and reduced cost. Improved security will benefit the customers as their privacy and fraud concerns are reduced while reduced costs may lead to cheaper communication costs for the customers.

The findings of the study will also benefit the shareholders of the telecommunications firms as it will lead to improved security reducing insecurity related costs while achieving the same at the most efficient costs. The reduction in the insecurity will lead to lower insurance premiums and

losses. These will in turn lead to better earnings per share and therefore more in come and more assured continuity for the business in the long-run.

This study also enables the communications authority of Kenya which is a key stakeholder in the communications industry as the regulator to understand the dynamics of the corporations' choices on corporate security management strategies and therefore inform the authority's decisions in the exercise of its' regulatory mandate.

The study will enable the Communications Authority of Kenya to determine and give guidance to the corporations on the strategies expected of them to meet the set standards of security. The study established that some strategies ensure better security compared to others and therefore should be adopted to increase security for both the corporations' infrastructure and intangible assets as well as safeguard customer privacy issues from being exploited by criminals in security related incidents.

1.6 The Scope of the Study

This study was conducted on corporations in the telecommunications industry in Kenya; Safaricom, Airtel and Orange. Primary and secondary data was used to evaluate the relationship between the security management strategies and profitability. This study targeted corporate security practitioners in the two levels of corporate security practice; security governance level and management level working for the three telecommunications corporations based within Nairobi County. This study evaluated corporate security management strategies metrics that affect profitability of the corporation for the time period 2011-2016. The time period selected for this study is the latest block of six consecutive years whose financial books have been audited and the

lengthy period enabled the study to build actuarial data from the estimates especially in the calculation of ALE. The research targeted the firms' facilities in Nairobi County.

1.7 Limitations of the Study

The entire target population was somehow biased towards their preferred strategy. However, secondary data was used to mitigate the effect of the bias in self-reporting.

The instrument employed in the data collection posed a challenge as some security practitioners were adamant about putting security related information in writing on materials whose access restriction is not guaranteed. To mitigate this, this study captured data in the questionnaires in percentages and proportions to the extent that is possible and the promise of keeping the raw data collected from the specific individuals under restricted access.

1.8 Organization of the Study

This research project was structured as follows: chapter one bears the research background, research objectives, research hypothesis, significance of the study, the scope of the study and the anticipated hindrances in the course of the study. Chapter two presents the literature review on the corporate security management strategies and profitability on the Kenya telecommunications firms. Chapter three presents the methodology engaged in the study for collection, analysis and presentation of the data. Chapter four presents the findings of the study and interpretation. Chapter five gives the summary conclusions as well as recommendation for the study.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction to Literature Review

Corporate security has over time metamorphosed from a fridge routine 'watchman' work to a core corporate management function with a role in the assurance of business continuity. Theories have been postulated to define the role of corporate security function and its' benefit to any given organization. Different scholars and management gurus have also identified different strategies a given organization may employ in managing its security function depending on the organizational goals, values, culture and future plans. The literature relating to this emerging key corporate management function is reviewed under two broad aspects namely; theoretical assessment and the empirical study.

2.2 Theoretical Review

Dealing with a multiplex operating domain is costly and can considerably thwack a corporation's profitability. Safeguarding the financial state and solidity of a corporation is a key issue for management. The supervening pressures from handling the bottom line are a rich etymology of challenges for numerous ventures throughout the corporation, particularly for security management (Carelli, 2009). It is for this reason that various theories on the value of corporate security have been postulated. The mitigation value theory states that the value of corporate security can be determined by evaluating the value a corporation gains from having a corporate security capable of deterring the occurrence of security incidences.

The revenue potential theory postulated by Georg (2007) states that corporate security may have revenue potential depending on the customers' evaluation of its perceived duty of care. If the

ascertained duty of care is more than zero, a yield potential for the corporation theoretically subsists.

"External Function of Corporate Security (EFCS) theory" evaluates the role corporate security plays in deriving value out of the perception of the stakeholders. It states that incase security breaches occur, and as a result there is failure, customers, financiers, and shareholders will punish the given corporation using a myriad of tools and implements at their disposal (Eisenhardt, 1989).

Internal Function of Corporate Security (IFCS) theory evaluates the value of corporate security as a function of the inner workings of the given corporation. It involves the actual and direct benefits of having a functional and effective corporate security. According to Georg (2007), IFCS elements include among others assessment of emerging security threats, standards and certifications.

2.2.1 Mitigation Value Theory

Mitigation value theory states that the biggest value of corporate security is its ability to mitigate incidences that would otherwise affect the business in a negative manner (Ritchey, 2012). This theory seeks to identify the value of corporate security by evaluating the benefits gained from the prevention of adverse security concerns. If for example a business whose customer base reduced by a given percentage in a year where a given percentage change in security related issues were experienced. If this would lead to an increase in number of customers, then the value of that customer increase could be considered as an impact of security on profitability as it affects the overall revenues.

Addressing security concerns so that they are prevented before they happen instead of addressing them after they happen makes a corporation seem more attractive to customers. This attractiveness

to customers leads to an increase in business. The converse leads to loss in business which also translates to lose of profits for the corporation (Stafford, 2007).

Georg (2007) identified the structure below as the initial construct of corporate security

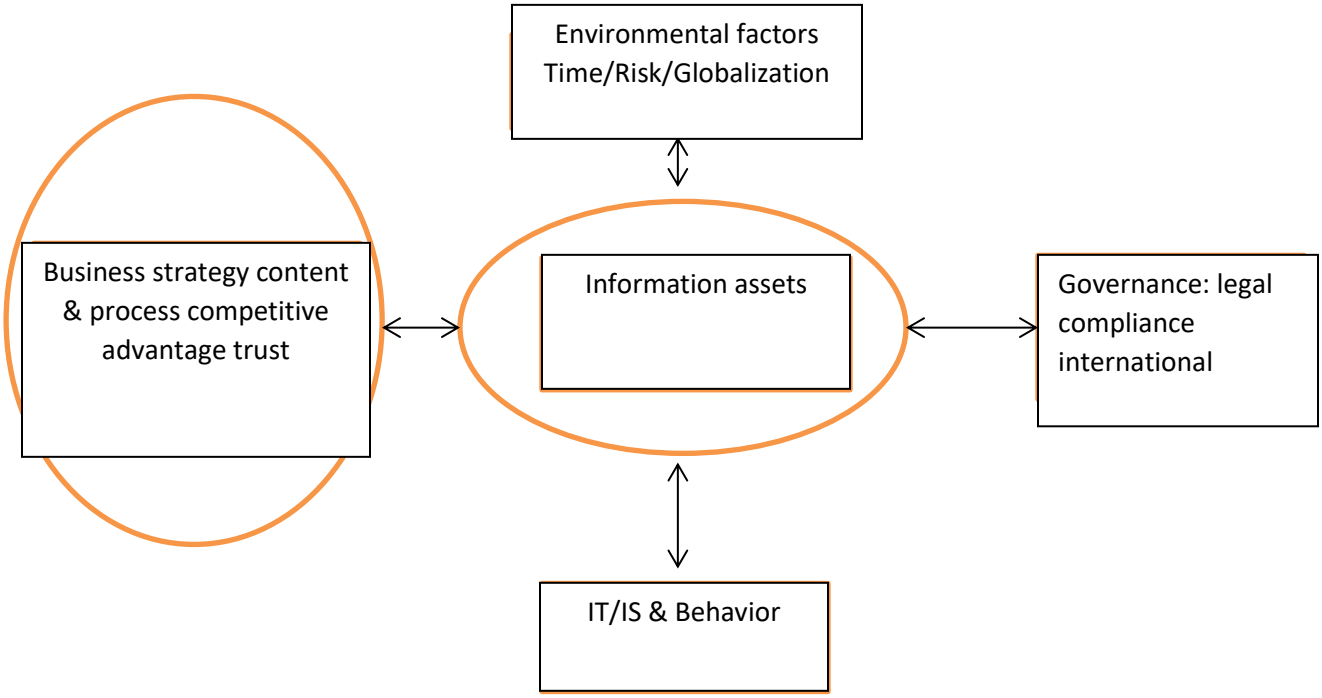

Figure 2.1: Initial Corporate Security Construct for Mitigation Value

Source: Georg 2007

Security is a business stumbling block that should be formulated and disentangled in the backdrop of the corporation's strategic drivers (Carelli, 2009). The corporations' strategic drivers seek to derive advantage from tackling business challenges before their onset or having a plan to deal with them way ahead of time. Similarly, adequate preplanning on security helps the organization to develop and grow advantage in being able to prevent occurrence of security incidences.

Security is so inextricably fastened to the triumph of the corporation in perpetrating its mission and bettering resilience that it is in the corporation's nonpareil engrossment to be masterly at

securing itself (Carelli, 2009). This in essence therefore implies that irrespective of the core function of any given organization or corporation, it is important that the corporation develops core competence in the area of securing itself. Corporations in the Kenyan telecommunications industry's core business are providing platforms for communication between people and other platforms and people. Despite that, it is important that the same corporations find a way of developing core competence in the area of security in order to ensure resilience in the medium and long-term.

In determining the scope of corporate security management in the Kenyan telecommunications industry, we have to identify the security challenges that they face. Security challenges could be categorized based on their effects on the fundamental security requirements such as confidentiality, integrity and availability of VOIP networks (Edelson, 2010). These aspects of security in the telecommunications industry are the most pertinent to the customers perceived privacy and therefore, goes a long way in influencing their spending in that organization.

Personnel security is the provision of a degree of affirmation as to the trustworthiness, probity, rectitude and reliability of labourers, contractors and temporary staff (Cabinet office, 2012). This is a key security concern for Telco's as their employees have access to infrastructure and information that if inadvertently accessed and or shared would be detrimental to the corporations' image and would cost them dearly an example is access to subscriber geographical locations, SMSs and call logs. That information if accessed and shared would cost the company its image for privacy concerns. In this specific aspect, there exists no clear-cut way to manage a breach of privacy and therefore all must be invested in preventing it.

Many corporations are embracing a risk-based approach to security. The shift to a risk-based paradigm is a catalyst for shifting security from a technical specialty to an organizational proficiency. Applying a risk outlook to security is a cerebral progression as risk management is a rudimentary business function. Whether it's undertaken implicitly or explicitly, it must be executed at an organizational level to be enterprising (Carelli, 2010).

Avoidance caused by customer's failure to trust the service provider leads to losses, an assurance to restore that trust because of the actions of corporate security leads to more spending on the specific Telco leading to better earnings and therefore better profitability. According to Yates insecurity is a big cause of reserved spending among customers that reduce the turnover of the company and therefore negatively affecting profits (Yates, 2003).

In the Kenyan telecommunications industry the revenue losses that maybe occasioned by the switching of mobile phones to avoid rogue service provider employees from accessing one's location details and passing them on to third parties the detriment of the subscriber may not be quantifiable but proper vetting of employees may actually lead to higher revenue. Avoidance behavior which is caused by lack of trust causes revenue losses (Stafford, 2007).

There are activities done by corporate security personnel that increase costs but some on the organization may not deem them as worth doing for example internal fraud and theft (Albrecht, 2001). However, on the other hand some corporations may perceive employee related theft as an unpreventable and unpleasant occurrence that is part of doing business.

However, since employee theft is unknown, the management may not be able to decide on the greater cost between catching a thief and accepting employee related theft as an inevitable

occurrence (Ibid:443). The acceptance of the employee related theft in a corporation could serve as an encouragement for the deplorable employee habit.

In order to establish if there exists a relationship between corporate security management strategies and profitability in the telecommunications firms in Kenya. It is imperative to understand how the value of security is determined using the mitigation value theory. This theory will be employed to determine metrics upon which revenue generated by corporate security can be quantified.

2.2.2 The Revenue Potential Theory

According to Georg (2007) whether corporate security can be considered to have revenue potential is dependent on a customer's evaluation of their duty of care. If this adjudged duty of care ($\dot{\varepsilon}_c$) is greater than zero, a yield latitude for the organization theoretically subsists; if it is zero, thus no reverence of care lies in the perspective of the customer within their own responsibility, no revenue can be precipitated for the organization. In essence therefore, the value of corporate security in terms of revenue to the organization is driven from the customer's perception of the need for security from that given corporation. In order to derive revenue from the corporate security function it must be empirically proved that the corporations target customers perceive a duty of care on their part. The more the revenue the corporation can draw from corporate security the higher the positive effect the function has on the corporation's profitability.

$\dot{\varepsilon}_c > 0 \rightarrow$ revenue potential

$\dot{\varepsilon}_c = 0 \rightarrow$ no revenue potential

The determinants of this boundary will differ from one industry to another. However, in the Kenyan telecommunications industry these will range from regulatory requirements, ethics to culture. This is because the government in Kenya is interested in the security of both the infrastructure, medium and interfaces given the key role communication plays in the economy. Georg (2007) further identified two other elements besides the sale of security services under the theory discussed above and includes reputation and trust.

This theory is key in guiding this study to establish value for corporate security. The existence of a revenue potential in the presence of perception of duty of care on the customer can be translated to revenue and therefore a factor in the calculation of the effect any of the given strategies affects profitability. The absence of security while there is a perceived duty of care on the part of the customer does also translate to cost of bad security which is vital in this study.

2.2.3 The EFCS Theory

The external function of corporate security (EFCS) is a theory which was postulated by (Eisenhardt, 1989). According to this theory, corporate security value can be looked at in the eyes of the stakeholders and the same could be quantified to check its effect on the corporation's profitability. Also known as reputation risk for a corporation, EFCS seeks to portray the corporation as a secure one. Accordingly, it is perceived as such and therefore it's able to attract the right investors in the securities exchange. The right investors consequently provide the corporation with cheaper credit facilities and business connections that are key in ensuring the corporation increases its revenues while at the same time ensuring that the costs remain manageable if reduction is unattainable.

The EFCS theory further suggests the existence of alignment of the internal and external functions of organizational security initiating a communication design between the clientele and the internal organizational security function. Better alignment between IFCS and EFCS ensures finer corporate risk appropriation as the corporation has a preferable discernment into customer security worries and hence help adjust its vulnerability evaluation (Georg, 2007). This alignment creates value for the corporation, a value that can be captured directly or indirectly to the profitability of that corporation.

The aspects of competitive intelligence, investor perceptions and the retail customer focus are factors of the EFCS. The corporation's security management must bear in mind that their functions influences how the three aspects of the stakeholders perceive the company. A corporation that is perceived to have a thorough security is perceived as one that has the ability to weather any challenge that it may face and therefore making it appear more stable. The stability leads to cheaper credit, more customers and competitors are demotivated to engage in corporate espionage.

Zulz (2015) indicated that the increase in security threats, mostly cyber-attacks to corporations will now be influencing Moody's ratings. A drop in the Moody's ratings is an undesirable feat for any organization because it signifies increase in risk and therefore lenders charge a higher risk premium when lending to that organization which in turn erodes the earnings and could derive the organization out of business. This signifies the need for organizations to keep their security perceivably effective as an external function.

This theory states that there is value in having effective security and therefore there is a cost to having ineffective security whether actual or perceived by the stakeholders. Accordingly, good security strategy has revenue and cost potentials which ultimately influence a given corporation's

profitability. By quantifying the costs and revenue under this theory this study will be enable to analyze how the external function of corporate security is monetized under the various management strategies and how each of these strategies influence this function.

2.2.4 IFCS Theory

Internal function of corporate security theory was put forward by Georg (2007) to define the value that is generated internally by the corporate security. Effective corporate security management can be exploited to generate revenue for the organization. The theories identify information security, physical security and the security of both employees and the premises from direct damage and theft as the aspects of internal function of corporate security. The actual security unlike the reputation and trust that defines the external functions of corporate security.

Eisenhardt (1989) identified the value driven from corporate security to be two-fold. To affect the corporate profitability, corporate security must have a cost or value that can be translated to revenue. Eisenhardt identified IFCS and EFCS as the two variable values of corporate security. He identified EFCS as the domain that is created around IFCS and where organizational security overlaps with the corporations' shareholders' concerns. In the event of insecurity or security related incidents that shine a light of incompetence on the part of corporate security, stakeholders that include customers, shareholders, financial investors and suppliers will badly punish that organization (Georg, 2007).

The responsibilities of corporate security must include protection of the people who work for the organization, protection of the organizations' property and the prevention of the organization from incurring liability (Kidd, 2010). The protection of the organization's employees and property as

well as shielding the corporation from liability and all other aspects involved in doing that is what is termed as the responsibility of corporate security management.

This theory goes further to identify risk management as a function of corporate security management. It suggests that the emergence of insurance may have curtailed this as a responsibility of the corporation's security management but corporations are taking note that corporate security performs a critical function in risk elimination, control and avoidance. "The role of protection on the part of corporate security not only cover a factory, equipment and structures but also items like commercially sensitive information, procedural secrets and information attained from costly research" (Blake, 2010). In the Kenyan telecommunications industry, some of the corporation's key competencies like Mpesa for Safaricom include some secrets that Safaricom would want to keep a secret from the rest of the industry players.

Internal function of corporate security theory postulates that the value of corporate security is in its internal value to the corporation. The actual protection and risk aversion in the corporation which translates directly into costs and revenue. According to (Georg, 2007) the internal function of corporate security consists of the risk evaluation of newly manifesting security threats for example internal fraud, hacking attempts, and also all other formal and informal security measures.

The measures that a corporation employs are mainly dependent on the security strategy that corporation has adopted. The measures a result of the security strategy impacts on customers' perception of the business which affects profitability. Introduced security measures may at times lead to a negative reaction, leading to a negative security dividend. The introduction of roll-down opaque security shutters may make customers perceive insecurity in that environment and therefore avoid shopping there (Willis, 1995).

The internal function of corporate security seeks to determine the value added to the profitability of a given organization by the actual security and the cost of bad security as a direct function of the profitability. This theory unlike the external function of corporate security theory does not evaluate how the perception of security in the corporation influences third parties who in return influence the profitability of the given corporation through trading in the stock market, credit pricing, bonds uptake and creditors faith.

Internal function of corporate security theory attributes the ability of the corporate security to the management of the direct security incidents and threats. For example, in a telecommunication corporation the function and the value of corporate security is the ability of the practice to stop the corporation from suffering losses as a result of pilferage in the shops, theft of cables both fiber optic, copper and aluminum cables

2.3 Empirical Review

Canton (2003) identified three strategies in corporate security management in the modern business environment. He identified them as contract security management strategy, proprietary corporate security management strategy and the combined proprietary and contract corporate security management strategies. The choice of which of the three strategies a given corporation adopts is dependent on several factors. The number of guard forces a corporation requires determines which strategy to adopt, for example large guard forces favor contract security over proprietary strategy (Walsh, 2003). Accordingly, the larger the number of security guards required the more the balance tilts away from proprietary security towards contract security strategy.

The nature of duties required of the corporate security also plays a role in determining what strategy is adopted. Simple duties can be performed by contract security with only a few hours of

site training. Complex duties however, require extensive training and past experience are performed best by in-house security (Canton, 2003). In the telecommunications industry in Kenya if the target responsibility is to guard the telecommunications masts in far flung areas from unauthorized access then that is a simple duty that does not require specialized training and therefore can be contracted. However, if the task is to guard the more complex infrastructure like servers in buildings with a lot of human traffic then those duties are complex and require very specialized training and this would therefore imply that proprietary corporate security management strategy is more appropriate.

The quality of available supervision, local job market and the budget requirements are also very key in determining the appropriate strategy to be adopted by a corporation according to Canton (2003). This therefore implies that corporations in the Kenyan telecommunications industry must consider these factors in making the choice of the corporate security management strategy to adopt.

A PwC study that surveyed more than 1,200 senior executives and board members in the US found that over the preceding 3 years, 55 percent of security management leaders recorded increased profit margins and 41 percent achieved an annual profit margin of more than 10 percent upon employment of good risk management strategies (Olavsrud, 2015).

Some forms of security management strategies help reduce risk of insecurity incidents by employing measures that lead to identification and forecasting of emerging risks, horizon scanning and early warning indicators and building organizational resilience to risk. According to the PwC study 46 percent of security managers spend more time calculating and preparing for security incidents than reacting to it as compared to 21 percent of non-managers. It further established that 96 percent vs 59 percent spend time in identification and forecasting of security incidents while

81 percent vs 33 percent spent time in scanning the horizon and early Warning indicators (Olavsrud 2015).

A study by Ngaari (2016) established that risk management does to only have a positive correlation with profitability of a given corporation but the relationship is also significant. The study also established a significant positive correlation between operational risk management and profitability in the banking industry.

A study by Challenger (2006) found out that the immediate impact of good security on the commercial health of a corporation is that it keeps the corporation's assets secure. The assets are therefore able to be utilized, the additional expenses involved in replacing them are avoided, and the possibly greater losses through loss of business or inability to service clients are forestalled. This study, however, did not go further and establish whether these forestalled losses and secured assets affected the profits of the given corporation.

A study on the effects of insecurity on profitability of companies working in the Niger Delta by Efeelo (2018) found out that there exists an inverse but significant relationship between number and magnitude of security incidences suffered by a company in an accounting year and the gross profit margin in the same period. Reduction in the gross profit margin is as a result of lost revenue due to services not provided to the customers as well as the cost of replacement of the facilities and equipment damaged or lost in the security incidences. A reduction in the gross profit margin means a reduction in profitability of that given corporation. The more the incidences the better the security management remedies required to address it and therefore the more the cost thereof.

The Niger Delta study further established that security related incidences further affected the operating profits of the companies by establishing an inverse but significant relationship between operating profits and security related incidents in a given accounting period.

Statistics show that the net expenditure by corporations on cyber security in the US rose from 27.3 billion dollars in the year 2010 to 54.8 billion in the year 2016 according to a research by the ITU (Gerami, 2017). These costs however, do not include those associated with other forms of security. Evidently, the costs are significant in any context and therefore affects the profits of the affected corporations.

Proper security management in a corporation can lead to increased revenue and not just a cost center in the traditional sense. According to Geer (2018), 73% of executives surveyed believe security risks are on the rise, only 12% of those are successful security risk management leaders. Over the three-year stretch leading to the study, 41% of that 12% produced an annual profit margin growth of more than 10%, according to the survey. Security risk management doesn't simply mitigate risk; it magnifies net income. Ostensibly, the difference in classification from those who consider it as a cost center to those who consider it as a profit magnifier signifies the role the strategy adopted plays in determining how it affects the profits of that given corporation.

Human Resource management strategies in a corporation impacts that given corporation's profitability. According to Lopez (2016), 60 percent of executives are beginning to see that Human Resource management can partner with other departments to increase the profitability and value of a business. The study established that good human resource management strategies gives an organization efficiency in the face of increased competition; it leads to more revenue from less expenditure and this increases profit margins in that organization.

The use of training and development strategies explains a significant 33.4% variance in profitability corporations in Kenya. While the use of reward and compensation strategies explains a 9.2% variance in profitability. This according to a study by Katua (2014) signifies the role Human Resource Management strategies plays in impacting the profitability of corporations in Kenya.

Empirical evidence exists of the relationship between other corporate management functions including finance management and Human Resource management and profitability of corporations in Kenya and beyond. Further studies have been done to establish the relationship of corporate security and profitability of organizations in the Niger Delta.

The telecommunications industry in Kenya is highly competitive and results in cost management to retain competitive advantage. Lower service costs lead to lower charges on the customers and better profit margins for the firms attracting more customers and more usage of their service by the customers (Edmunson et al, 2018). The study however, did not go as far as to establish whether the security management strategies played a role in the cost management or the profitability in a broader context.

With corporate security management having grown into a corporate management function like human resource is, and the Kenyan telecommunications industry being one of the fastest growing, contributing more and more to the GDP and being particularly prone to security related incidences that may cause a lot of damage to both equipment and reputation and consequently the profitability of the firms in that industry, a need existed to asses how the strategies adopted to manage security in those corporations impacts their profitability.

Dimension	What is done	What is needed to be done
Security risk management and profitability in the banking sector.	Ng'aari (2016) established a positive and significant relationship between security risk management and profitability in the Kenyan banking industry.	However, there hasn't been a study on relationship of the same variables in the telecommunications industry in Kenya
Corporate security and profitability in the Niger Delta.	Efeeloo (2018) established that corporate security management costs impact profitability of companies in the Niger Delta.	However, there hasn't been a study to establish the effect of security management for corporations in Kenya and more specifically in the telecommunications industry.
HRM strategies and profitability in the banking industry.	Katua (2014) established a positive correlation between human resource management strategies and profitability in the Kenya banking sector.	While corporate security management has grown into a corporate management function like the Human Resource Management and the telecommunications industry is just as competitive and impactful to the GDP, studies have not been done on

		how it affects profitability in the industry.
Cyber security management and profitability among US blue chip companies.	Geer (2018) established a positive and significant correlation between cyber security management strategies efficiency and business profitability in the US.	However, studies have no been done on the efficiency of corporate security management strategies in Kenyan corporations and especially those in the telecommunications industry in Kenya and how the same impacts profitability.
Competitiveness in the Kenya telecommunications industry.	Edmunson et al (2018) established a positive and significant correlation between cost per customer served by a telecommunication firm in Kenya and the company's profitability.	However, there has been no study to establish whether costs incurred in security management or security incidences impact on the overall cost and therefore profitability.

2.3.1 Proprietary Corporate Security Strategy and Profitability of the Telecommunications Firms in Kenya

Proprietary corporate security management strategy is the practice where a given organization directly employs its security personnel. This direct employment enables the given organization to control the hiring standards. The salary and other forms of emoluments are similar to those other employees in that organization. Any post-hiring training and professional development is the responsibility of that corporation.

Corporations can commit additional resources to substantial training of security practitioners and those practitioners are likely to feel more devoted to and therefore increasing their loyalty to the company (Bradford, 2009). Proprietary security as evidently pointed out by Bradford leads to more expenditure in terms of training. It however induces better loyalty to the corporation in the part of the security practitioners and therefore the corporation may be able to draw the benefits of an entirely loyal employee. In the Kenya telecommunications industry, the cost of training would translate to expenses on the corporation as the benefits of loyalty and better security services would lead to better provision of the security services by the security employees.

Selecting, training and supervising own security personnel is a key aspect of proprietary security. This costs more but guarantees better security services by the employees (Holden, 2010). The process of selecting and training costs Telco's a fortune in the case of proprietary security. However, the benefits of recruiting as per the corporation's high standards and human resource policies also has its benefits that can translate to value on the profit and loss account.

Security officers hired directly by a corporation can be more reliable (Barton, 2000). Barton established that proprietary security being direct employees of the company get company

sponsored training and standard the chance of advancement in the company to areas that are not security. This makes them more reliable and are unlikely to change workplaces too often for their experience to be useless.

Mcgee (2006) in his paper on the condition of corporate security and its potential for future professionalization identified security practitioners who formerly worked for the government performed better than those who didn't at least in the first few years of their work. This he said was due to the work ethic especially for those from the military as well as connections in the government security apparatus that give them an advantage. Most former government security practitioners are unlikely to be employed by security companies that second them to other organizations to offer security.

In-house security costs more that outsourced security per head as the wages will include other benefits, taxes and uniforms (Lanfranchi, 2000). In his research, Lanfranchi established that it costs more to maintain proprietary security than it costs to maintain outsourced security. The study however, considered aspects of the employment terms like vacations that were not quantified.

Holden (2000) identified the advantages of proprietary security as more control of the security personnel by the corporation as they are direct employees, loyalty and reliability. In-house security will provide a given organization loyalty, reliability and control which the corporation must find a way to translate into revenue directly or indirectly.

2.3.2 Outsourced Corporate Security Strategy and Profitability of the Telecommunications Firms in Kenya.

Outsourced security strategy also referred to as contract security is a security management strategy employed by some corporations and involves the contracting of a private security company to

provide security services. A firm enters into a contract with another firm that provides its employees to provide the security. Holden (2000) describes this management strategy as the taking up employees through a third-party organization.

A private security firm is paid an agreed amount of money periodically to provide security to the contacting corporation. The contract may specify the number of guards the private security firm should provide or it may just state the provision of security as the hired service leaving the number the private firm deploys to do so at the discretion of the of that private firm. The duties of the contracted security firm will vary depending on the contract and rages from provision of just personnel to providing both personnel, equipment and other resources required by the corporation to ensure security. The contract may go as far as shifting the cost of any security related issues to the contracted firm (Lanfranchi, 2000).

Contracted security firms offer flexibility at an affordable price (Canton, 2003). Due the flexibility of this strategy, an organization need not keep extra security personnel on the payroll for a day circumstances might need more security personnel without adequate planning time. This strategy enables an organization to only pay for the number of security personnel it needs on a day to day basis and does not need to consider the possibility of having one to cover while the other is on vacation, sick or attending to other emergencies.

According to Holden (2000), a firm contracted to provide security almost always has security equipment for use therefore saving the contracting firm from high capital expenditure. This equipment may include those used for deployment of the security personnel in far flung premises and installations as well as those needed for alarm response. This enables the corporation to amortize a fraction of the costs over a period of time. Outsourcing security also enables the

corporations to spread risk and liability for selection, training and actions of the security officers between them and the contracted firm.

The training costs, recruitment, supervision and payroll management are costly endeavors in the security function that in the outsourced security function are incurred by the contracted firm saving the contracting organization (Lanfranchi, 2000). The costs associated with these tasks in borne by the contracted firm saving the contracting firm. Besides the direct expenses like the advertising and the stationery used in these tasks there are other hidden costs like wages for human resource staff involved in the recruitment as well as the man hours of the management used in the recruitment.

Canton (2000) established that there are costs to having lowly paid employees seconded to an organization. These costs include those that are arise due to poor morale, lack of commitment, disloyalty and propensity to engage in other activities to bridge the earnings difference. He also identified contract management costs as one that is often overlooked in analyzing the cost of contracting security.

2.3.3 Hybrid corporate security strategy and Profitability of the Telecommunications Firms in Kenya

In many organizations according to George (2000), only the base grade security services are contracted. In their research in the UK they found out that the mix between contract and proprietary security changed a lot in five years as corporations sought the mix that gave them the best return on investment. They found out that there exists a major hidden cost in contract security in the

management of that contract. Without the contracting firm closely managing the contract, the contracted firm may get away with providing services of lesser quality.

This is the corporate security management strategy that is defined by a mix of both proprietary security and outsourced security. Both proprietary and outsourced security has specific advantages and shortcomings as a result some corporations choose a mix between the two that offers the advantages of each while mitigating the shortcomings of the other (Holden 2000).

Not all security positions require the same abilities. Some guards will perform simple duties while others will perform complex duties. By combining the strengths of both the contract and proprietary security, it is theoretically possible to achieve a cost-effective mix that minimizes the weaknesses of both (Canton, 2003). In its most basic form, hybrid security strategy involves the contracted personnel performing the simpler tasks while the more complex ones are left for the in-house security. Some organizations with highly trained but few proprietary security may augment them with contracted security because of their flexibility.

Some organizations employ this strategy such that the supervisors are proprietary while the guards are contracted. This enables them to rotate the guards often enough to avoid collusion between them and employees. This was specially employed by Zale Corporation Distribution Centre in New York. The Pacific School of Dentistry in San Francisco and the Community College of Pennsylvania were identified by Lucien (2003) as having employed this to maximize the ROI of the corporate security function.

2.3.4 Profitability

Profitability in any industry is the ability of any player in the industry to get a a positive return on any given investment. Corporations in every industry are today faced by more competition that at

any other point in the past. As a result, companies have been forced to stream-line personnel-related support functions such as security to increase their return on investment for a competitive edge (Lanfranchi, 2000). Every strategy therefore must be gauged against its impact on the given corporation's profitability where the basic concept is maximizing the return on investment by finding the balance that gives the best returns per dollar of investment.

Every business understands security is an inexorable expense and this is evidenced by the fact that all corporations seek to keep their premises secure (Challinger, 2010). All corporations must operate in financially responsible way which includes the protection of assets. The stakes stoked on corporate security have grown since the function moved from mere egress control to include physical security, personnel security, information security, security education and awareness training, investigations, business continuity, counter fraud and evaluation.

"The broadening purview of security risk is necessitating security departments align with the core organizational goals, a move that is also about how to successfully shift from 'security as a cost' to 'generating benefits from security'" (ASIS International, 2010). Whether security is viewed or implemented as a cost center or value center the cost and the value will impact on the profitability of the given corporation for which the security is employed offer services whether proprietary, contracted or a combination of both.

A set of entrenched and embraced metrics for quantifying security ROI, which can be employed by a corporation in itself by performing computation in the context of security event avoidance or effect of the realized threat whose effect charge is comparatively lower than control therefore leading to positive consideration (Carelli, 2010). There is one way in which the impact of corporate security on profitability is determined and that is ensuring the cost of a pre-realized risk is

determined and the cost of the control and the difference between the two will determine whether the impact is positive or negative on the profits of that organization.

A corporation that prosperously captures security as a venture may expand its overall portfolio in the market place and might also be able to seize the profit as goodwill on their balance sheet. While goodwill on a balance sheet may not translate directly into profits, in the long run corporations will leverage this accumulated goodwill of the corporations for profits through improved balance sheets leading to cheaper and readily available credit. A corporation whose security strategy assures its balance sheet remains healthy leads directly and indirectly to the improvement of the profitability of that corporation according to (Carelli, 2010).

By precisely quantifying the costs of security infringements whose repercussions are pilferage and prudently documenting recoups made, it is feasible to provide statistics which empower top management to comprehend what the manifestation of corporate security can do for the bottom-line (Kidd, 2010). The reason why a knowledge gap exists in determining the relationship between corporate security management strategies and profitability, is the absence of an agreed upon formula to determine the actual benefits of security in monetary terms. However, Kidd suggests a way of determining the contribution by valuing the difference in costs of security breaches.

The existence of good and effective security in a corporation improves its employee retention rate because workers prefer working in safety and this has the financial benefit of employee retention. “One study in 2000 found that the annual cost of employee turnover in the supermarket sector overshoots industry net earnings by 40%” (Meyer, 2000). In the telecommunications industry careful security assessment and insecurity mitigation will lead to savings in employee turnover costs.

Figlio (2002) viewed corporate security as a loss prevention programme whose fundamental objective should be to convincingly demonstrate a feasible return on investment in the security programmes. This involves the identification of the problems that would have occurred had the organization not adopted and invested in the corporate security as it did in that case.

PricewaterhouseCoopers established that EAS systems installed in retail outlets to lower stock theft had a sound ROI based on the figures from stock shrinkage (DiLonardo, 2003). The return on investment of security programmes can be quantified by evaluating the losses prevented by the installation or investment in security systems and programmes against the amount of money invested in the system in both wages and capital expenditure by the organization.

Profitability is a function of revenue and expenditure. This study will establish costs related to the various corporate security management strategies by identifying the costs of attributable to security and then it will be used to establish the cost of security under each of the three strategies per head of security and then per unit area of premises secured. The costs that will be considered will include; average hourly pay rate, overtime premium rate, vacation pay, paid holidays, paid sick leave, payroll taxes, worker compensation insurance, medical cover, liability and property damage, recruitment costs, uniform and equipment and the cost of contract and contract management costs (AlliedBarton, 2000).

To calculate profitability as a function of corporate security, the study will determine the Annual Loss Expectancy (ALE) of the given firms. To calculate ALE, the company will establish the Single Loss expectancy (SLE), the Annualized Rate of Occurrence (ARO) and the Exposure Factor (EF).

$$ROI = \left(\frac{ALE}{COST\ OF\ COUNTERMEASURES}\right) X\ 100\%$$

$$ALE = SLE\ X\ ARO$$

2.4 Summary and Research Gap to be filled

Research has been done on the role of corporate security, its evolution and growth from a peripheral department to a main corporate function. The professionalism of the practitioners and the emergence of the private security firms have also been researched on by researchers across the world. Some researchers have also identified the various corporate security management strategies practiced across the world and how each of the strategies differ from each other. Research has also identified the cost centers associated with the various strategies and the benefits attributable to each.

Considering the fact that every corporations' bottom-line is to enhance profits through maximizing return on investment and seeking to assure business continuity especially in this era of cut-throat competition in the telecommunications industry in Kenya. There exists a gap in available research on how each of the different corporate security management strategies affects the profitability of the given corporation.

The identification of the various costs associated with the various corporate security management strategies alone does not help organizations make informed choice of strategy considering the bottom-line. The costs particular to every strategy and the associated revenue have not been compared against each other on how they impact the profitability of the given organizations.

2.5 Conceptual Framework

The conceptual framework in the figure below manifests the relationship between the independent variables, the dependent variables and the intervening variables.

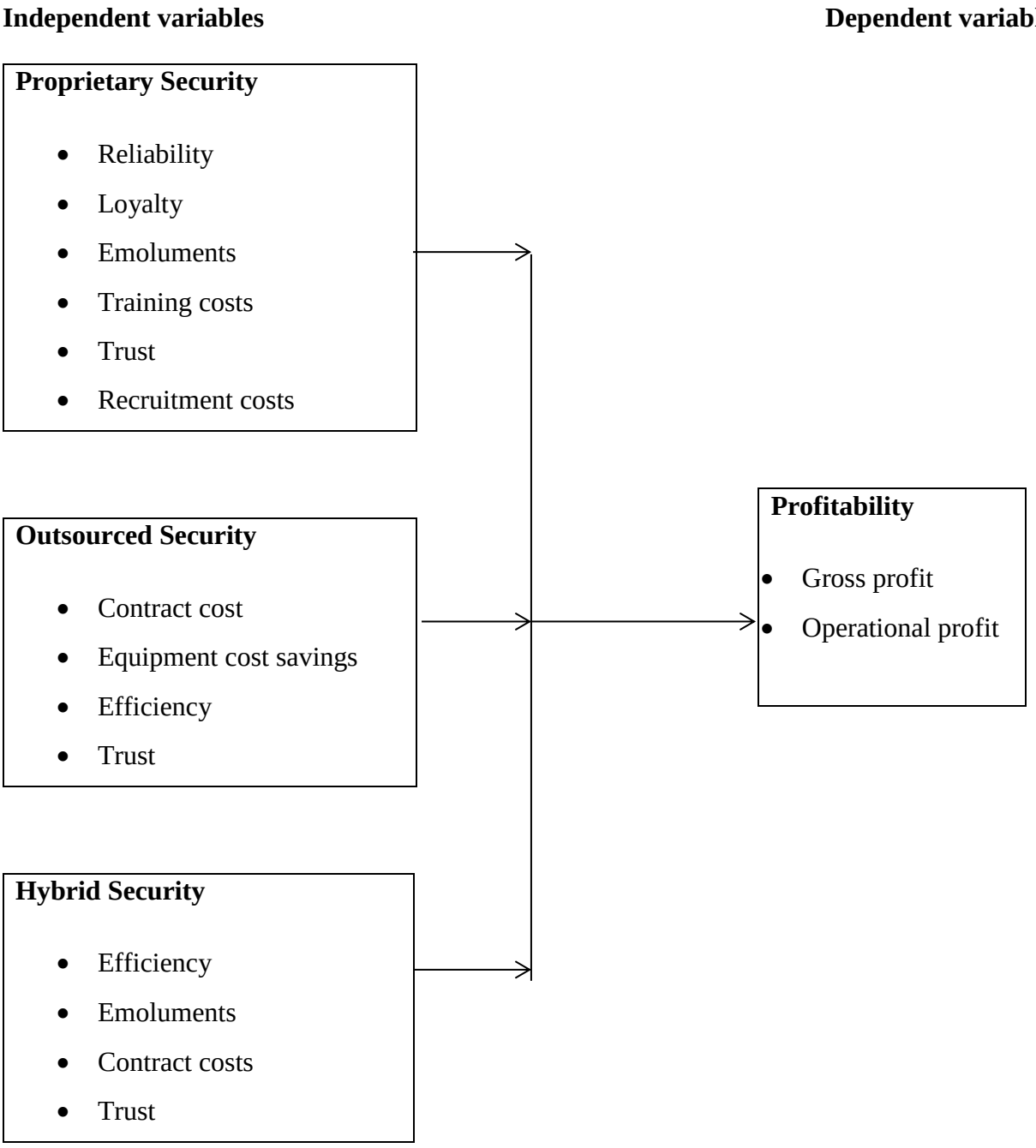

Figure 2.2 Conceptual Model

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter proffers the research methodology that was employed in this study. It sheds more light on the research design, target population, sampling procedures, instrumentation and data collection techniques analysis and presentation.

3.2 Research Design

Longitudinal survey model was used in this study. Longitudinal survey is a research design in which information is collected through interviews or the administration of questionnaires to a sample of persons (Orodho, 2003). This research design enabled the collection of data for the study from the target population on the implications corporate security management strategies has on the profitability of the various corporations in the Kenya telecommunications industry over a period of the five years under study. This research design enabled the study to establish if there really exists a relationship between corporate security management strategies and profitability and the kind of relationship it is.

3.3 Target Population

The target population of this study was the corporate security practitioners in the Kenya telecommunications sector. This industry consists of Safaricom, Airtel, Orange and Equitel as the main players during the period under study. This study however did not consider Equitel, a service provider that has limited infrastructure as it borrows into another service provider's infrastructure. The targeted security practitioners in the three corporations in the Kenya telecommunications industry are in two cadres' namely security governance and line management level. The study

targeted those personnel in Nairobi county-based facilities. A total of 67 security practitioners at the management and governance levels were employed by the three telecommunications firms in Nairobi as at the time of the study.

Table 3.1: The Target Population

Corporation	**Governance level**	**Management level**
Safaricom	6	27
Airtel	4	15
Orange	3	12
Total	**13**	**54**

Source; Security Practitioners of Kenya (2017)

3.4 Sampling Design

Granted the population in this study is small and all the respondents were efficiently being reached out to give the data required the study employed census sampling procedure. In this case therefore all the 13 managers at corporate governance level and 54 line managers adding up to 67 managers were considered for the study.

3.5 Data Sources and Collection Instruments

Primary and secondary data were collected and utilized in this study. The primary data was principally gathered through the administration of a questionnaire. “Questionnaires are one of the best tools for data collection in research” (Mugenda and Mugenda, 2008). The nature of corporate security makes it even more appropriate for data collection in this study as compared to other instruments. Each questionnaire had two parts; part one consisted of questions to establish the

personal status of the respondent while part two consisted of questions on corporate security strategy, cost and discernable revenue streams associated with the strategies.

Secondary data was acquired from annual financial reports of the corporations. The secondary data collected from the financial reports enabled the study obtain data that cannot be obtained from the practitioners. The secondary data obtained from the financial records were the profits of the various telecommunications firms during the period under study.

3.6 Data Collection Procedure

Data was acquired by use of a questionnaire which was administered through email for the respondents in the governance while personal drop and pick method was used for management level. This is because respondents in the governance are not always physically and readily available due to commitment in various places from where they are to access such a questionnaire physically.

3.7 Validity and Reliability

Validity is the extent to which a concept is accurately measured in a quantitative study while reliability relates to the consistency of a measure. This study employed a pilot study to establish the validity and reliability of the instruments used.

3.7.1 Pilot Study

Pilot study is usually done to establish the suitability of the research instruments. It assists in detecting inadequacies in the instrument before the real study is undertaken (Orodho, 2008). In this contemplation, pre-testing of this study instrument was done in 10% of the sample but was not incorporated in the actual data collected for the study. The pre-tenting enabled the research to be validated. The pre-tenting also made sure that the instruments were reliable for the purpose of

collection of precise and detailed data. Accordingly, the validity and the reliability of instruments used in this study was determined as follows. According to Connelly (2008), extant literature suggests that a pilot study sample should be 10% of the sample projected for the larger parent study.

3.7.2 Validity of the Study Instruments

Validity alludes to the expanse to which an instrument measure out what it is expected to measure, data does only need to be reliable but should also be veracious and accurate. If a quantification is sound, it is also dependable (Mugenda & Mugenda, 2008). To make certain that validity of the instruments for this study, content, appearance and construct validity was given thought to. Face or appearance validity alludes to the research's impressionistic examination of the presentation and appropriateness of the research instruments (Oluwatayo, 2012). To ensure that the instruments are relevant, sensible and clear, experts were consulted in the area of descriptive research. Moreover, in the interest of ensuring that the instruments have content validity the experts were consulted. To ensure construct validity, the coherence of the items and the language degree of the research instruments was reflected on as a result of the pilot study.

To determine the validity of the data collection instruments, the research instruments was given to 10% of the sample size or 5 respondents were involved in determining validity and they were uniformly spread across the strata. They were required to offer their responses to exhibit how easy they can reply to the instruments in the study. The validity of the questionnaire was also determined to ascertain the questionnaire captured the content required for the study.

3.7.3 Reliability of the Study Instruments

Reliability refers to the consistency, dependability or stability of the data collected. Whenever a researcher measures a variable, they want to be certain of the dependability and consistency of the results provided by the measurement. A measurement should be able to provide consistent outcomes each time after several measurements for it to be considered reliable. Should the results differ, then the measurement cannot be relied on (Creswel, 2012). An analysis of the data obtained was done, after two weeks, the same instrument was re-administered to the same respondents. Subsequently, the first and the second attempts were compared. In determining reliability of research instrument Cronbach alpha (α=0.7) was applied where results revealed α>0.7 showing that instrument was reliable.

3.8 Data Analysis and Presentation

Analysis of the collected data was done using quantitative techniques. Data was coded, sorted and classified upon collection. Descriptive statistics were utilized in the analysis of the data where frequencies and percentages were used. Also mean was used to analyze the cost of proprietary security management strategy on profitability, the cost of outsourced security as well as the cost of hybrid corporate security management strategy. The mean was also used in analyzing the revenue generated for the corporation by the corporate security management strategies. In the qualitative data analysis, themes and categories emerging from the data were identified.

The research further employed a multiple regression model to assess if the independent variables of the security management strategies in predicting the dependent variable; profitability. The multiple regression model equation:

$Y = a + b_1X_1 + b_2X_2 + b_3X_3$

Where; y = estimated profit,

c = constant,

b = regression coefficient also known as beta coefficient and

X_{1-3} = the security management strategies.

This study used the ANOVA test model to analyze the inferential statistics. The ANOVA test utilizes the comparison of the means between groups of interest to determine whether any of the means have any statistically significant difference from each other (Laerd, 2000). Each corporate security management strategy was considered as a group. The difference between the cost and revenue (contribution) associated with each strategy was determined and the mean calculated.

$$H_0: \mu_1 = \mu_2 = \mu_3$$

Where μ_1= the mean contribution of proprietary corporate security management strategy μ_2 =the mean contribution of outsourced corporate security management strategy. μ_3 = the mean contribution of hybrid corporate security management strategy. If this test indicates a result that is significant statistically, then the alternative hypothesis is accepted. Should the p-value be greater than 0.05 ($p > 0.05$) then the null hypothesis (H_0) is true. However, if the p value is less than 0.05 ($p < 0.05$) then the alternate hypothesis (H_A) is true.

3.9 Ethical Considerations

In the process of carrying out this study a number of ethical concerns were anticipated and measures were taken to ensure that they were addressed and mitigated in line with academic research ethics. To ensure objectivity in this study all data analysis and interpretation was done using scientific methods and tools. All data, results, ideas, tools and resources used or obtained in

the conduct of this study will be openly shared in the spirit of openness as long as there is absolutely no reason to believe the same could be used to the detriment of the respondents or the corporations in the target industry. All information filled in the questionnaire and obtained in oral interviews was held in confidence and as such respondents were asked not to inscribe individual names on the questionnaires. All the participants in the study were required, expected and facilitated to act with integrity, carefulness, honesty, respect and within the law during the study.

Before the collection of data, a letter of authorization was obtained from the University and used to procure the Research permit from the National Commission for Science, Technology and Innovation (NACOSTI), a pre-requisite for conducting studies in Kenya.

CHAPTER FOUR

DATA ANALYSIS, INTERPRETATION AND PRESENTATION

4.1 Introduction

In this chapter, data on the relationship between corporate security management strategies and profitability in the telecommunications industry in Kenya will be presented. This study was led by the following objectives: to examine the effect of using proprietary corporate security management strategy on profitability in the telecommunications industry in Kenya, to establish the implications of outsourcing corporate security management strategy on profitability in the telecommunications industry in Kenya and to establish the implications of hybrid corporate security management strategy on profitability in the telecommunications industry in Kenya.

4.1.1 Response Rate

The study managed to collect data from 57 respondents out of the targeted sample of 67 which represented a response rate of 85%. To achieve this, frantic efforts were made to reach the targeted respondents through constant emails and telephone calls reminding them of the questionnaires. According to Souse (2008) if the rate of response is above 50%, then, it is sufficient for analysis; consequently, with a rate of response at 85%, it is sufficient for analysis in this study. The results are as shown in the Table 4.1.

Table 4.1: Response Rate

Response rate	Frequency	Percentage (%)
Responded	57	85
Not responded	10	15
Total	**67**	**100**

Source: Survey data (2018)

4.2 General Information

4.2.1 Gender

The study sought to determine the respondents' genders and their spread. The study determined that a majority of the respondents working in these companies are male as shown by 62% while only 38% of the respondents are female. The dominance of men among the respondents can be attributed to the Kenyan traditions and culture where security jobs are viewed as man-like. These walls are however coming down as women transcend the cultural and traditional barriers as well as the broadening of the security sector jobs to include the non-physical security jobs especially in the field of cyber security (RoK, 2008). The results are as shown in the Table 4.2.

Table 4.2: Gender

Gender	Frequency	Percent (%)
Male	35	62
Female	22	38
Total	**57**	**100**

Source: Survey data (2018)

4.2.2 Age Bracket

The study targeted to establish the respondents age brackets. It was determined that those in the age bracket 41 – 50 years were the majority among the respondents as manifested by 51% trailed by the 32% in the age bracket 31-40 years, trailed by those above 50 years manifested by 10% of the respondents, whereas those under the age of 30 constituted just 7% of the respondents. This implies that top management jobs comprise of adults with vast experience. Barney (2001) opines that skills, responsibilities and experience come with age. Sixty per cent of the respondents happen to be in the age considered the most active and a time of maturity. Consequently, the findings

indicate that the telecommunication corporations are led by capable and mature leadership who can be instrumental in the sustainable stewardship of their organizations. The results are as shown in the Table 4.3.

Table 4.3: Age bracket

Age bracket	Frequency	Percentage (%)
Under 30 years	4	7%
31-40yrs	18	32%
41-50	29	51%
Above 50years	6	10%
Total	**57**	**100**

Source: Survey data (2018)

4.2.3 Level of Education

The education levels of the respondents were determined by the study. The research established, the majority of the respondents had bachelor education as show by 51%, trailed by 32% of the respondents who had masters education as their lofty academic qualification, then Diploma as manifested by 11% and finally 6% of the respondents with PhD as their academic qualification. This indicates that most of the managers who head security in the telecommunication industry have high levels of education to steer their business and also have the knowledge about the different functioning of their business. Nassimbeni (2001) opines that entrepreneurial and managerial skills of most entrepreneurs are influenced by academic qualifications. The onus of educational learning as an agent of change cannot be disputed. Values and skills transmission for the stimulation of social modification and societal sustenance has always utilized education as a central transmission mechanism. The results are as shown in the Table 4.4.

Table 4.4: level of education

Level of education	Frequency	Percent (%)
Diploma	7	11%
Bachelor	29	51%
Master	18	32%
PhD	3	6%
Total	**57**	**100%**

Source: Survey data (2018)

4.2.3 Position Held

This section of the research sought to find out positions the respondents held in the organizational hierarchy. The study established that 36% of the respondents were marketing managers; followed by 20% of the respondents who were heads of security departments, 18% were finance managers, 15% were human resource managers whereas only 11% were in the board of governors. This indicate that majority of the respondents are conversant with security details of the organizations and matters finance or effects security details has on firm profitability. The results are as tabulated in the Table 4.5.

Table 4.5: Position held

Position held	Frequency	Percent (%)
Human resource manager	9	15%
Finance manager	10	18%
Head of security department	11	20%
Marketing managers	21	36%
Board of governors	6	11%
Total	**57**	**100%**

Source: Survey data (2018)

4.2.4 Years of experience

This bit of the research sought to establish the years of experience of the respondents. The research determined that most of the respondents as manifested by 53% had between 6 and 10 years of experience, this was followed by 28% of the respondents who had worked for over 10 years in their organization, this was followed by 20% of the respondents who had worked in their

organizations for between 2 and 5 years. None of the respondent had worked for less than one year. The results indicate that the respondents had vast knowledge about their organization and could give information required by the study. The results are as tabulated in the Table 4.6.

Table 4.6: Years of Experience

Level of education	Frequency	Percent (%)
Less than one year	-	-
2-5 years	11	20%
6- 10 years	30	52%
Above 10 years	16	28%
Total	**57**	**100%**

Source: Survey data (2018)

4.2.5 Corporate Security Management Strategies

This bit of the study sought to determine the corporate security management strategies the telecommunication companies have had in the past six years. The study established that all the companies have had proprietary, outsourced and hybrid options for their corporate security management strategies in the last six years.

4.3 Data Reliability

The assessment of the degree to which a research instrument yields homogenous data or result after replicated trials is termed as data reliability (Malhotra 2014). The cardinal formula for establishing reliability based on internal consistency is Cronbach alpha (α) (Kim & cha, 2002). Conceptual elements used in this research were put to test for internal consistency dependability using Cronbach alpha (α) test. According to Malhotra (2014) the standard minimum value is 0.7. The study adopted a composite Cronbach's alpha that exceeded the cut-off value of 0.70. The measures were composed of items with response choices that ranged from 5 ("strongly agree") to 1 ("strongly disagree").

Proprietary corporate security management: Proprietary corporate security management was measured using the six items . Proprietary corporate security management had a Cronbach alpha (α) of 0.834.

Outsourcing corporate security management: Local resources mobilization was measured using four items anchored on a five-point Likert scale. For all measurement scales, standardized Cronbach's alpha was examined. Outsourcing corporate security management had Cronbach alpha (α) of 0.781.

Hybrid corporate security management: Hybrid corporate security management was measured using four items anchored on a five-point Likert scale. Hybrid corporate security management got Cronbach alpha (α) of 0.745. The results of the reliability statistics and measures of all variables are summarised and presented as tabulated in the Table 4.7.

Table 4.7 Cronbach Alpha Coefficient for the Variables

Variable	Cronbach's Alpha	No. of Items
Proprietary corporate security management	0.834	6
Outsourcing corporate security management	0.781	4
Hybrid corporate security management	0.745	4

Source: Survey Data, 2018

4.4 Effect of Using Proprietary Corporate Security Management Strategy on Profitability

4.4.1 Years when the business had proprietary corporate security

This bit of the study sought to determine between which years the business engaged proprietary corporate security. The study revealed that the business engaged proprietary corporate security between different years. The study revealed that Safaricom employed proprietary corporate security between 2012 and 2015, Airtel employed proprietary corporate security between 2013

and 2015 whereas orange employed proprietary corporate security between 2012 and 2013. The results are tabulated in Table 4.7.

Table 4.7: Years when the business had proprietary corporate security

Telecommunication firms	Years for Proprietary Corporate Security
Safaricom	2012-2015
Airtel	2013-2015
Orange	2012-2013

Source: Survey Data, 2018

4.4.2 Number of security personnel

This bit of the study sought to establish the number of security personnel the organizations had. The study revealed that Safaricom had the most security employees in Nairobi county with 45% of the total security employees by the firms in the telecommunications industry in Kenya, this was followed Airtel with 28% and lastly Orange with 27%. The results are as shown in Table 4.7.

4.7: Number of security personnel

Telecommunication firms	Frequency	Percent (%)
Safaricom	140	45%
Airtel	86	28%
Orange	84	27%
Total	**310**	**100%**

Source: Survey data (2018)

4.4.3 Attending Training

This section of the study sought to establish how often the security personnel attend trainings. The research determined from a majority of the respondents that they attend training on weekly basis as shown by 43% followed by 30% of the respondents who revealed that their security teams attend training on monthly basis, this was followed by 17% who revealed that they attend training on daily basis whereas 10% revealed that they rarely attend trainings. The results are tabulated in Table 4.8.

Table 4.8: Attending Training

	Frequency	Percent (%)
Daily	10	17%
Weekly	24	43%
Monthly	17	30%
Rarely	6	10%
Total	**57**	**100%**

Source: Survey data (2018)

4.4.4 Rate Recruitment and Training and Equipment Costs

This section of the study sought to rate costs associated with recruitment, training and equipment involved in proprietary security. The research determined that from a majority of the respondent that it was costly as manifested by 40% followed by 30% who said it was fair, followed by 20% of the firms that reported that it was very costly, finally only 10% of the firms reported that it was cheap. Similar study by Bradford (2009) revealed that corporations can consign more resources to security employees' professional training which in return would be expected to encourage the employees to be more loyal and more invested in the corporation. Proprietary security as evidently pointed out by Bradford leads to more expenditure in terms of training. It however induces better loyalty to the corporation in the part of the security practitioners and therefore the corporation may be able to draw the benefits of an entirely loyal employee. The results are as tabulated in Table 4.9.

Table 4.9: Rate Recruitment and Training and Equipment Costs

Degree	Frequency	Percent (%)
Cheap	6	10%
Fair	17	30%
Costly	23	40%
Very costly	11	20%
Total	**57**	**100%**

Source: Survey data (2018)

4.4.5 Annual Total Wages for the Security Department

This bit of the study sought to establish the average annual cost attributable to proprietary security per head. The study revealed that 88% of the security practitioners under proprietary security were paid below Kshs 1,000,000 per annum, followed by 9% who earned between Kshs 1,000,001 and Kshs 5,000,000, whereas only 3% earned above kshs 5,000,000 per annum. The results are as tabulated in Table 4.10.

Table 4.10: Annual Total Wages for the Security Department

Annual total wages	Frequency	Percent (%)
Below 1,000,000	274	88%
1,000,001 - 5,000,000	28	9%
Above 5,000,000	8	3%
Total	**310**	**100%**

Source: Survey data (2018)

4.4.6 Rating statements on proprietary security

This section of the study sought to establish how the respondents agreed to statements relating to proprietary security. Likert scale was adopted in carrying out this evaluation of statements relating to proprietary security. The scale span from 1 to 5 where 1=strongly disagree, 2=disagree, 3=neutral, 4=agree 5=strongly agree. The study established that proprietary corporate security strategy is highly reliable with a mean of 4.02 agreeing; security workers are loyal, a mean of 3.62 was revealed manifesting that they agree; there are low emoluments, a mean of 2.32 was revealed manifesting that they disagree; there are low training costs, a mean of 2.57 was revealed showing that they disagree; workers are trustworthy, a mean of 4.22 was revealed manifesting that they agree and there are low recruitment costs, a mean of 2.34 was revealed showing that they disagree. Similar studies by Bradford (2009), revealed that employees who are trained and have confidence in their skills are more loyal to the corporation and they are more efficient in the performance of their duties and therefore more resources directed to training increases efficacy. Proprietary

security as evidently pointed out by Bradford leads to more expenditure in terms of training. It however induces better loyalty to the corporation in the part of the security practitioners and therefore the corporation may be able to draw the benefits of an entirely loyal employee. In the Kenya telecommunications industry, the cost of training would translate to expenses on the corporation as the benefits of loyalty and better security services would lead to better provision of the security services by the security employees. The outcome is tabulated in Table 4.11.

Table 4.11: Rating statements on proprietary security

Statement	Mean	Std dev
It is highly reliable	4.02	.568
Security workers are loyal	3.62	.745
There are low emoluments	2.32	.874
There are low training costs	2.57	.564
Workers are trustworthy	4.22	.451
Low recruitment costs	2.34	.452

Source: Survey data (2018)

4.5 The Implications of Outsourcing Corporate Security Management Strategy on Profitability

4.5.1 Years on outsourcing corporate strategy

This bit of the study sought to determine the years that the firms engaged outsourcing corporate security. The study established that the companies utilized outsourcing corporate security between 2014 and 2016.

4.5.2 Cost per year on outsourced security

This bit of the study sought to establish the annual cost of contracting security per year per head. It established that 98% of the contracted security earned below Kshs 1,200,000 per annum, 2% earned between Kshs 1,200,001 and Kshs 5,000,000 while nobody was contracted to earn more than Kshs 5,000,000 per annum. The outcomes are as tabulated in Table 4.12.

Table 4.12: Cost per year on outsourced security

Annual total wages	Frequency	Percent (%)
Below 1,200,000	182	98
1,200,001 – 5,000,000	4	4
Above 5,000,000	-	-
Total	**186**	**100%**

Source: Survey data (2018)

4.5.3 Rating Factors on Outsourcing Security

This section of the study sought to rate how different factors relating to outsourcing corporate security strategy are true or otherwise. In carrying out this task the study employed a scale of 1 to 5 where 1=strongly disagree, 2=disagree, 3=neutral, 4=agree 5=strongly agree to rate the different factors. The study revealed that on contract cost is low, a mean of 4.25 was revealed showing they agree; there is a lot of saving costs on equipment, a mean of 4.62 was revealed showing they agree; outsourcing brings about efficiency, a mean of 4.34 was revealed showing they agree; trust is enhanced through outsourcing security, a mean of 3.22 was revealed showing they are neutral. Similarly, according to Holden (2000), a firm contracted to provide security almost always has security equipment for use therefore saving the contracting firm from high capital expenditure. This equipment may include those used for deployment of the security personnel in far flung premises and installations as well as those needed for alarm response. This enables the corporation to amortize a fraction of the costs over a period of time. Outsourcing security also enables the

corporations to spread risk and liability for selection, training and actions of the security officers between them and the contracted firm. The outcomes are as tabulated in Table 4.13.

Table 4.13: Rating Factors on Outsourcing Security

Statement	Mean	Std dev
Contract cost is low	4.25	.854
There is a lot of saving costs on equipment	4.62	.785
Outsourcing brings about efficiency	4.34	.452
Trust is enhanced through outsourcing security	3.22	.641

Source: Survey data (2018)

4.6 The Implications of Hybrid Corporate Security Management Strategy on Profitability

4.6.1 Years Hybrid Security Was Employed

This section of the study sought to determine the years in which the telecommunication companies employed hybrid corporate security management strategy. The study established that hybrid security was employed between the years 2015 and 2016.

4.6.2 Rating hybrid security

This section of the study sought to rate how different factors relating to hybrid security are true or otherwise. In carrying out this task the study employed a scale of 1 to 5 where 1=strongly disagree, 2=disagree, 3=neutral, 4=agree 5=strongly agree to rate the different factors. The study revealed that efficiency is enhanced, a mean of 4.04 was revealed showing they agreed; emoluments are low, a mean of 3.67 was revealed showing they agreed; contract costs are low, a mean of 4.37 was revealed showing they agreed and trust is enhanced through hybrid system, a mean of 4.04 was revealed showing they agree. Similarly, the Pacific School of Dentistry in San Francisco and the Community College of Pennsylvania were identified by Lucien (2003) as having employed hybrid

to maximize the return on investment of the corporate security function by mixing both proprietary and outsourcing corporate security strategy. The results are tabulated in Table 4.14.

Table 4.14: Rating hybrid security

Statement	**Mean**	**Std dev**
Efficiency is enhanced	4.04	.745
Emoluments are low	3.67	.894
Contract costs are low	4.37	.771
Trust is enhanced through hybrid system	4.04	.459

4.7 Profits

This section of the study sought to establish profits that were made by the telecommunication companies since 2012 to 2018. The study found the following from financial data. The results are tabulated in Table 4.15.

Table 4.15: Profits

Company/year	**Safaricom (billion)**	Airtel **(billions)**	**Orange (billions)**
2012	12.63	2.64	1.43
2013	17.5	3.67	1.99
2014	31	6.61	3.53
2015	31.9	6.69	3.63
2016	38.1	8.0	4.34
2017	45	9.45	5.13

Source: Survey data (2018)

4.8 Inferential statistics

To test the relationship between the variables (independent and dependent), this research employed a multiple regression analysis. To enter, code and compute the mensuration of the multiple regressions, this study employed the statistical package for social sciences (SPSS V21).

The extent to which changes on the part of the dependent variable are logically explainable by changes on the part of the independent variables or the percentage variations in the dependent variables that can be justified by one or all the independent variable (proprietary, outsourcing and hybrid security strategies) is described by the coefficient of determination.

4.8.1 Model Summary

The three independent variables studied, explained only 19.3% of out-turn of different security costs strategies on financial performance as represented by R^2. Consequently, this means factors other than those researched in this study contribute 80.8% on profitability. Accordingly, further research needs to be done to probe the other factors (80.8%). The results are tabulated in Table 4.16.

Table 4.16: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.438	.192	.182	.60880

Predictors: (Constant), proprietary, outsourcing and hybrid security

Source: Survey data (2018)

4.8.2 ANOVA Results

The significance value at 0.0214 is less than 0.05 and therefore, the model is significant statistically in forecasting how proprietary, outsourcing and hybrid security affects profitability of telecommunication companies in Kenya. The F critical at 5% level of significance was 0.95579. The results are tabulated in Table 4.17.

Table 4.17: ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2.553	28	0.0918	0.94579	.0224
	Residual	9.413	97	0.0940		
	Total	**11.966**	**125**			

Predictors: (Constant), proprietary, outsourcing and hybrid security

Dependent variable: Profits

Source: Survey data (2018)

4.8.3 Regression Coefficients

To determine the relationship between corporate security strategies and the profitability of telecommunication companies in Kenya a multiple regression analysis was conducted. The SPSS generated table 4.7, the equation ($Y= a + B_1 X_1 + B2 X_2 + B_3 X_3 + \epsilon$) develops to:

The Multivariate regression model Becomes:

$Y= 1.2371B + 0.195 X_1 + 0.308X_2 + 0.335X_3 + e$

According to the regression equation, the study determined that taking all factors into account (proprietary, outsourcing and hybrid security) constant at zero, the profitability of the corporations will be 1.2371B. The findings proffered also shows that assuming all other independent variables at zero, a unit enhancement in proprietary security rates lead to a 0.185 pecuniary amplification of

telecommunication corporations; a unit rise in outsourcing security levels lead to a 0.308 pecuniary amplification of telecommunication corporations; a unit increase in hybrid security leads to a 0.335 rise in the financial profitability of telecommunication companies in Kenya. This surmises that hybrid security has the most contribution towards the financial profitability trailed by outsourcing security. At 95% level of confidence and 5% level of significance, proprietary security strategy had a 0.0239 level of significance; outsourcing strategy exhibited a 0.0224 level of significance hybrid exhibited a 0.0217. The mitigation value theory has similar view on that a combination of business mitigation mechanisms/measures has a positive effect of raising the business performance. The biggest value of corporate security is its ability to mitigate incidences that would otherwise affect the business in a negative manner (Ritchey, 2012). In an organization that spreads its risks through a number of security cost portfolios this leads to stability of profits and therefore enhancing stakeholder's confidence and therefore overall good performance of the organization.

Addressing security concerns so that they are prevented before they happen instead of addressing them after they happen makes a corporation seem more attractive to customers. This attractiveness to customers leads to an increase in business. The results are tabulated in Table 4.18.

Table 4.18: Regression Coefficients

	Unstandardized Coefficients		Standardized Coefficients	
Model	B	Std. Error	Beta	Sig.
(Constant)	1.2371	6.686		.0359
proprietary	.195	.388	.255	.0239
outsourcing	.308	.531	.395	.0224
hybrid	.335	.425	.002	.0217

a. Dependent Variable: Profitability

b. predictors: (proprietary, outsourcing and hybrid security)

Source: Survey data (2018)

4.9 Hypothesis Testing

4.9.1 H_{01}. There exists no relationship between proprietary corporate security management strategy and profitability in the telecommunications industry in Kenya.

The results of the research revealed the relationship strength between proprietary corporate security management strategy and profitability is 0.195 that was significant at .0239 confidence level; this therefore dismisses the assumption that there exists no relationship between proprietary corporate security management strategy and profitability in the telecommunications industry in Kenya.

4.9.2 H_{02}. There exists no relationship between outsourced corporate security management strategy and profitability in the telecommunications industry in Kenya.

The results of the study revealed that relationship strength between outsourcing corporate security management strategy and profitability is 0.308 which was significant at .0224 confidence level; this therefore dismisses the assumption that there exists no relationship between outsourcing corporate security management strategy and profitability in the telecommunications industry in Kenya.

4.9.3 H_{03}. There exists no relationship between hybrid corporate security management strategy and profitability in the telecommunications industry in Kenya.

Resulting from the study, the strength of relationship between hybrid corporate security management strategy and profitability is 0.335 that was significant at .0217 confidence level; this therefore dismisses the assumption that there exists no relationship between hybrid corporate security management strategy and profitability in the telecommunications industry in Kenya.

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This bit of the study presents the summary of the findings, conclusions and also the recommendations of the study.

5.2 Summary of the findings

5.2.1 Proprietary Corporate Security Management Strategy and Profitability

The research found that proprietary security strategy is reliable, the security workers are loyal and trustworthy. However, the emoluments, training costs and recruitment costs are high. The results of the research revealed that the strength of relationship between proprietary corporate security management strategy and profitability is 0.195 that was significant at .0239 confidence level; this therefore dismisses an assumption that there exists no relationship between proprietary corporate security management strategy and profitability in the telecommunications industry in Kenya.

5.2.2 Outsourced corporate security management strategy and profitability

The study also established that with outsourcing security strategy; contract costs are low, there are saving on training, equipment and also efficiency is enhanced though trust is not optimal.

The results of the research revealed that the strength of relationship between outsourcing corporate security management strategy and profitability is 0.308 that was significant at .0224 confidence level; this therefore dismisses the assumption that there exists no relationship between outsourcing corporate security management strategy and profitability in the telecommunications industry in Kenya.

5.2.3 Hybrid corporate security management strategy and profitability

The study finally established that with hybrid security system; efficiency is enhanced, emoluments are low, contract cost is low though trust and reliability are sub-optimal especially in the areas with the contracted security personnel.

The results of the research revealed that the strength of relationship between hybrid corporate security management strategy and profitability is 0.335 which was significant at .0217 confidence level; this therefore dismisses the assumption that there exists no relationship between hybrid corporate security management strategy and profitability in the telecommunications industry in Kenya.

5.3 Conclusions

The study concluded that proprietary security system is costly though it guarantees trust and reliability both scoring a mean of 4.22 and 4.02 on the Likert scale respectively. The proprietary system also has positive and significant effect on profitability of the telecommunication companies as manifested by the profits reported by the firms during the time the strategy was in use.

The study also concluded that outsourcing corporate security strategy is cheaper in-terms of salaries and overall contract costs as signified by the mean score of 4.24 on the Likert scale. The study also concluded that there exists positive correlation between outsourcing security strategy and profitability of telecommunication companies as the study revealed a relationship strength of 0.195 significant at .0239 confidence level.

Finally, the study concluded that hybrid security strategy is cheaper compared to proprietary security as shown by the mean score of 4.37 on the Likert scale. The study also found a significant

positive correlation between hybrid security strategy and profitability of telecommunication companies with the strength of the relationship at 0,335 significant at .0217 confidence level.

5.4 Recommendations

5.4.1 Study Recommendations

The research recommended to the top management of the telecommunication corporations to evaluate their business models well based on the different benefits as well as drawbacks with the different options for strategic security. They may choose proprietary security management strategy for its reliability and trust and choose to suffer higher emoluments, training and equipment related costs that have effects on profitability or go for the other forms and have low contract costs which have direct positive effect on profits but less trust and reliability.

The study further recommends the employment of the hybrid corporate security management strategy as it offers the most efficient balance between the need to cut security related costs while at the same time ensuring the firms do not suffer detrimental losses arising from unreliability of the cheaper options. A fine blend between the Proprietary security and the outsourced security offers the most economical approach where critical areas as well as the senior security staff are under Proprietary security, while the routine egress control responsibilities are outsourced.

The study recommends that private security companies contracted to provide security services underwrite the losses of a portion of them occasioned by the unreliability of their staff to in offering security services to improve their reliability and trustworthiness.

5.4.2 Recommendations for further studies

This research also recommends that a further research be conducted to establish if sourcing of security personnel from the same labor pool at different costs (expensive in proprietary and less costly in outsourced security) has an effect on the reliability of security services offered by both.

The research also recommends for a comparative study to be done on the financial implications of security strategy choices across the East africa.

REFERENCES

Adum, O. A., Nkolika, O. E., & Ezeokana, J. O. (2006). *Current Trend in Social Science and Management Thoughts*. Enugu, Nigeria: John Jacobs Classic.

Albrecht, G., & Searcy, M. L. (2001). Insignificant Security Breaches vs Cost of Corporate Security. *Security Management Journal Vol 57.*

Aljawarneh, S. (n.d.). Cloud Security Engineering Concept and Vision. *Cyber Security and Threats*, 93-101. doi:10.4018/978-1-5225-5634-3.ch006

AlliedBarton, (2000, Oct). The three Corporate Security Management Strategies and how they affect competence. AlliedBarton Magazine, 167.

ASIS International. (2010). *Risk Analysis and the Security Survey 4th Edition*. Atlanta, Georgia: ASIS International.

Barney, J. B. (2001). Resource-based Theories of Competitive Advantage: A ten-year Retrospective on the Resource-based view. *Journal of Management.*

Barton, T. L. (2000). Understanding Corporate Security in the 21st Century: The Birds eye view perspective. *Journal for Security Management Vol 10.*

Barton, T. L. (2002). A Dynamic National Security Strategy: Creating Synergy Between Strategy, Forces, and Resources. *Journal for Security Management Vol 16.*

Baskerville, P. (1990). Canadian Papers in Business History. *Labour / Le Travail*, 26, p.247.

Baskerville, R. (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems,1*(2),

Blake, W., & Clarke, S. (2010) Risk Management as a Corporate Security Responsibility rather than an Insurance Matter. *International Journal of Corporate Security Vol 7.*

Bradford, P. (2009). *The Logic and Limits of Trust.* New Brunswick: Rodgers University Press,

Briggs, R., Edwards, C., & Pickard, J. (2006). *The business of resilience: corporate security for the 21st century*. London, England: Demos.

Buddie, J., Cavanaugh, E. R. (2011). Risk Management in Telecoms in Emerging Economies. *Africa Security Journal Vol 27.*

Building Consensus Through Risk Assessment and Management of the Department of Energy's Environmental Remediation Program. (1994)

Byington, J. R., & Mcgee, J. A. (2006). Data Security and the Cloud. *Journal of Corporate Accounting & Finance, 25*(5)

Calder, M.L. (2007). Raising the Bar for Security Professionals. *Security Journal vol 13.*

Caldwell, R. (2003). The Changing Roles of Personnel Managers: Old Ambiguities, New Uncertainties. *Journal of Management Studies,40*(4), 983-1004.

Campbell, E., Murphy, P.E. (2011). The Chief Security Officers' Dashboard. *ASIS International Journal Vol 4.*

Canton, L. (2003). Disaster Planning and Management: Does One Leadership Style Work for Both?. *Journal Of Leadership Studies*, *7*(3), 47-50. doi: 10.1002/jls.21297

Carelli, M. D., & Becker, H. (2009). *A new look at the relationship between school education and work: second all-European Conference for Directors of Educational Research Institutions, Madrid, 11-13 September, 1979*. Lisse: Swets & Zeitlinger.

Challinger, Y., Chan, C. (2010) *Competing Through Information Security in the Information Age.* London: Oxford University Press

Contract vs. In-House Security - AlliedBarton. (n.d.). Retrieved March 30, 2017, from http://www.bing.com/cr?http%3a%2f%2fwww.alliedbarton.com%2fPortals%2f0%2fNews%2fContractSecurityVsInHouseWorkingwithExpertsforSpecializedServices.pdf&p=DevEx,5061.1

Creswel, J. W. (2012). Research Design. Qualitative, Quantitative and Mixed Methods approach. *Sage Publications Academic Journal.*

Dalton, G. (2003). Corporate Reputastion with Regard to Security: Should you Mind Yours? *California Management Reviw 143*.

Data Cleansing. (2013). *Corporate Security Organizational Structure, Cost of Services and Staffing Benchmark*, 53-54.

Deitelhoff, N., & Wolf, K. D. (2010). Corporate Security Responsibility: Corporate Governance Contributions to Peace and Security in Zones of Conflict. *Corporate Security Responsibility*, 1-25.

Doeksen, A., &Symes, D. (2015). Business Strategies for Resilience: The Case of Zeeland's Oyster Industry. *SociologiaRuralis,55*(3), 325-342.

Edelson, N. R. (2000) *Telecommunications: The Industry of the Future*. Cambridge: Cambridge University Press.

Edmunson K., Bates, P. & Stephan, P. (2018). *Telecommunication competition market*

study in Kenya. Nairobi, Kenya.

Efeeloo, N. (2018). *Insecurity Costs and Profitability of Construction Companies in Nigeria's Niger Delta Region*. European Journal of Accounting, Finance and Investment. Vol.4, No.9; 2018.

Eisenhardt, Kathleen, M. (2000) Building Theories from Case Study Research. *Academy of Management Review Journal Vol 14.*

Employers' Liability and Workers' Compensation. (2012).

Figlio, D. N. (2002). *A Study of the Institutionalization of Formal Security Knowledge in Training.* Chicago, University of Chicago Press.

Geer, M. G (2018). *Impact of Cyber Threats on Business Profitability:* ITU Centres of Excellence Network for Asia-Pacific Region.

General security risk assessment. (2003). Alexandria, VA: ASIS International.

Georg, L. (2004) The Functions of Corporate Security Within Large Organisations. *Pierre ALLAN*

jounal vol 1.

George, B. D. (2000). *Research Training for Social Scientists*, London: SAGE publications.

Halibozek, E. P., &Kovacich, G. L. (2017). The Corporate Security Profession. *The Manager's Handbook for Corporate Security*, 65-74. doi:10.1016/b978-0-12-804604-3.00004-9

Holden, K. (2000). What do Information Security Standards say? *Computer and Security 27 No.5.*

Intellectual property in the public sector research base, cabinet office report,. (1993). *Computer Law & Security Review,9*(4), 186.

Johnstone, G. (2005). Research Ethics in Criminology. *Research Ethics,1*(2), 60-66.

Katua, T.K (2014). *Effect of Human Resource Management Strategies on the Performance of Commercial Banks in Kenya.*

Kelly, L. (2010). Where security feeds value (how information security can improve profitability). *Strategic Direction,26*(11).

Kidd, W., & Czerniawski, G. (2010). *Corporate Security Responsibilities: What to Protect in a Corporation. London: Sage Publications.*

Krehnke, M., &Krehnke, D. (2000). Configuration Management. *Information Security Management Handbook, Four Volume Set*.

Laerd, V. A. (2000). Testing for Normality Using SPSS Statistics. *Laerd Statistics, Vol 14.*

Lanfranchi, K., Liebenau, J. (2000) *International Perspectives on Information Security Practices, Opinions and tools,* London School of Economics and Political Science Vol 13.

Lee, A. S. (2006). A Scientific Basis for Rigor and Relevance in Information-Systems Research. *London School of Economics Journal Vol 18.*

Lee, C., Lindup, H. (2002). The Legal Duty of Care-A Justification for Information Security. *Information Security Bulletin 13, No.2.*

Lefler, R. (2013). Aligning Security Services with Business Objectives. *Aligning Security Services with Business Objectives,* 1.

Legal Aspects of ISs Security and Privacy. (n.d.). *Managing Information Systems Security and Privacy,* 137-150.

Legal Drivers for Corporate Security Intelligence. (2015). *Corporate Security Intelligence and Strategic Decision Making,* 53-74.

Lindup, K. (1994). The cyberpunk age. *Computers & Security,13*(8), 637-645.

Lippert, R. K., &Walby, K. (2014). Critiques of Corporate Security: Cost, Camouflage and Creep. *The Handbook of Security,* 881-899.

Lucien, G. (2003). Return On Investment for Corporate Security. *The international Journal of Corporate Security Vol 11.*

Mackenzie, Kelvin Calder . (2007). *Whos Who*. doi:10.1093/ww/9780199540884.013.25892

Malhotra, N., Franco, A., & Simonovitis, G. (2014). Publication Bias in Social Sciences: Unlocking the File Drawer. *The Science Journal, Vol 345, Issue 6203.*

Manunta, G. (2000). Is Security Utilitarian? *Security Journal,13*(2), 49-58.

Manunta, G. (2000). The Management of Security: How Robust is the Justification Process? *Security Journal,13*(1).

McGee, A. (2006). A Profile of Current Practices, Rewards, Responsibilities and Attitudes. *The UK Security manager,* 44.

Meerts, C. (n.d.). Corporate Security. *Corporate Security in the 21st Century*.

Metian, M., & Tacon, A. (2003). Satisfying the Feed Demand of Aquaculture: Reviews in Fisheries Science & Aquaculture. *Feed Matters Journal Vol 23.*

Meyer, H. (1998). Attacks spur detection efforts. *Computers & Security,17*(5), 407.

Meyer, J. (2000). The Cost of Employee Turnover on Business and its relation to Security Related Issues. *The British Security Journal Vol 36.*

Moresh, N. (2002). Internet Privacy and Security: An Examination of online trading. *Journal of Public Policy and Marketing vol 19, No. 1.*

Moses, R. (1995). Corporate risk analysis and management strategies. *European Convention on Security and Detection*.

Mugenda, A. (2008). Social Science Research: Theory and Principles. *Applied Research & Training Services.*

Mugenda, O. M., &Mugenda, A. G. (2005). Research Methods: *quantitative and qualitative approaches.* Nairobi, Kenya: African Centre for Technology Studies.

Mugenda, O. M., Hira, T. K., & Fanslow, A. M. (1990). Assessing the causal relationship among communication, money management practices, satisfaction with financial status, and satisfaction with quality of life. *Lifestyles Family and Economic Issues, 11(4),* 343-360.

Nalla, M. K. (2001). Designing an introductory survey course in private security. *Journal of Criminal Justice Education,12*(1), 35-52.

Nga'ari, E. W. (2016) *Effect of Risk Management Practices on the Profitability of Listed Commercial Banks in Kenya.* KCA University. Nairobi, Kenya.

Nassimbeni, G. (2001). Strategic and Operational Choices for Small Subcontracting Firms: Empirical Results and an Interpretive Model. *International Journal of Operations and Product Management.*

Oluwatayo, J. A. (2012). Assessment of Computer Literacy of Secondary School Teachers in Nigeria. *Journal of International Education Vol 8.*

Orodho, J. A., &Njeru, E. H. (2003). Access and participation in secondary school education in Kenya: *emerging issues and policy implications.* Nairobi, Kenya: institute of Policy Analysis & Research.

Petersen, K. L. (n.d.). The Politics of Corporate Security and the Translation of National Security. *Corporate Security in the 21st Century*.

Prentice, P. (2005). *Security in Business Strategy.* Boston. Harvard Business School Publishing

Ritchey, V., Smith, H. (2012). Risk Management and Corporate Security: A Viable Leadership and Business Solution Designed to Enhance Corporations in the Emerging Markets. *Computer and Security Vol 14.*

San, P. (n.d.). Rethinking Human Security. *Rethinking Human Security*, 5-6.

Security Management. (2009). *Security for Telecommunications Network Management*.

Sennwald, G., & Santa, D. D. (2003). Le raccourcissement du cubitus en baïonnette, indications, techniques et résultats. *Chirurgie De La Main, 25*(3-4), 136-140. Doi:10.1016/j.main.2006.03.008

Smith, C. L., & Brooks, D. J. (2013). Concept of Security. *Security Science*, 1-22. Doi:10.1016/b978-0-12-394436-8.00001-1

Stafford, M & Chang, L. (2007). Beyond Concern-Beyond the Value Mitigation. *Journal of Information and Management Vol 57.*

Stokes, R. (2004). Rethinking Corporate Security in the Post 9/11 Era. *Security Journal,17*(3), 65-66.

Thai, V. V. (2014). Solving the Security-Trade Puzzle. *Journal of Applied Security Research,9*(3), 305-327.

The handbook of security. (2017, January 18). Retrieved March 30, 2017, from http://www.worldcat.org/title/handbook-of-security/oclc/62782288

Wakefield, A. (n.d.). Corporate Security and Enterprise Risk Management. *Corporate Security in the 21st Century*.

Walby, K., &Lippert, R. K. (2014). Introduction: Governing Every Person, Place, and Thing — Critical Studies of Corporate Security. *Corporate Security in the 21st Century*, 1-13.

Walsh, C. E. (2003). *Monetary Theory and Policy, 3rd Edition.* Massachusetts Institute of Technology Press.

Willis, K. (1995). Imposed Structure and Contested Meanings. *Australian Journal of Business Management Vol 30 Issue 3.*

Yates, K. R. (2003). *The Concept of Corporate Security, 3rd Ed. Homewood.* Homewood Printing Press.

Zulz, A.H., Rudolph, K.M., & Jocelyne, K.M. (2015) Cyber Crime Surveillance. *International Journal on Security Management Vol 3.*

APPENDICES

Appendix One: Letter of Introduction

DENIS KAIREMIA,

Kenyatta University,

0723982973

Dear Sir/Madam,

Am pursuing a master degree in the area of business administration and currently doing my project to enable me to complete my studies. In this regard, I request you to assist me in filling this short questionnaire that takes around fifteen minutes, am doing a research with the title ‘the relationship between corporate security management strategies and profitability in the telecommunications industry in Kenya’. Your support is highly appreciated.

Yours Sincerely,

DENIS KAIREMIA

Kenyatta University

Appendix Two: Questionnaire

SECTION A: DEMOGRAPHIC DATA

1. Gender

   Male ( )

   Female ( )

1. Age bracket

   Below 30 years ( )

   31-40 years ( )

   41-50 years ( )

   Above 50 years ( )

2. Level of education

   Diploma ( )

   Bachelor ( )

   Masters ( )

   PhD ( )

3. Position Held

   Human Resource Manager ( )

   Finance manager ( )

   Marketing manager ( )

   Head of security department ( )

   Boards of governor ( )

   Others (Please specify) ( )

4. For how long have you been working in this organization?

   Not more than 1 year ( )

   2- 5years ( )

   5- 10 years ( )

   Above 10 years ( )

5. Please indicate if you have had the following corporate security management strategies in the last six years?

I. Proprietary ( )

II. Outsourced ( )

III. Hybrid ( )

SECTION B: EFFECT OF USING PROPRIETARY CORPORATE SECURITY MANAGEMENT STRATEGY ON PROFITABILITY IN THE TELECOMMUNICATIONS INDUSTRY IN KENYA.

6. Between which years did you have proprietary corporate security

   2012-2014 ( )

   2014-2016 ( )

   2016-2018 ( )

7. How many security personnel do you have in your organization ……..

   Below 10 ( )

   11-20 ( )

   21-30 ( )

   31-40 ( )

   Above 40 ( )

8. How often do they attend training?

   Daily ( )

   Weekly ( )

   Monthly ( )

   Rarely ( )

   Not at all ( )

   6. How would rate recruitment and training and equipment costs (a) cheap (b) fair (c) costly (d) very costly

   7. What is the Annual total wages for the security department providing proprietary security in kshs…….

   Below 1,000,000

   Between 1,000,001 -5,000,000

   Above 5,000,000

8. Do you think it is a big burden on your financial budget?

Yes no

9. Using a scale of 1 to 5 where 1=strongly disagree, 2=disagree, 3=neutral, 4=agree 5=strongly agree, please indicate the extent to which you agree to the following key indicators relating to proprietary corporate security management

Statement	**1**	**2**	**3**	**4**	**5**
It is highly reliable					
Security workers are loyal					
There are low emoluments					
There are low training costs					
Workers are trustworthy					
Low recruitment costs					

SECTION C: THE IMPLICATIONS OF OUTSOURCING CORPORATE MANAGEMENT SECURITY STRATEGY ON PROFITABILITY IN THE TELECOMMUNICATIONS INDUSTRY IN KENYA

10. Between which years did you have outsourcing corporate security?

2012-2014 ( )

2014-2016 ( )

2016-2018 ( )

12. What has been you cost per year on outsourced security Kshs…….

Below 1,200,000

Between 1,200,001 -5,000,000

Above 5,000,000

13. Using a scale of 1 to 5 where 1=strongly disagree, 2=disagree, 3=neutral, 4=agree 5=strongly agree, please indicate the extent to which you agree to the following key indicators relating to outsourcing corporate security management

Statement	1	2	3	4	5
Contract cost is low					
There is a lot of saving costs on equipment					
Outsourcing brings about efficiency					
Trust is enhanced through outsourcing security					

SECTION D: THE IMPLICATIONS OF HYBRID CORPORATE SECURITY MANAGEMENT STRATEGY ON PROFITABILITY IN THE TELECOMMUNICATIONS INDUSTRY IN KENYA

14. Between which years did you have hybrid corporate security in your organization?

2012-2014 ( )
2014-2016 ( )
2016-2018 ( )

16. Using a scale of 1 to 5 where 1=strongly disagree, 2=disagree, 3=neutral, 4=agree 5=strongly agree, please indicate the extent to which you agree to the following key indicators relating to hybrid corporate security management

Statement	1	2	3	4	5
Efficiency is enhanced					
Emoluments are low					
Contract costs are low					
Trust is enhanced through hybrid system					

SECTION D: PROFITS

Please indicate the profit in the following years

2012 ---------- 2013---------- 2014----------

2015 ---------- 2016---------- 2017----------

2018 ----------