RISKS AND RISK MITIGATION MEASURES IN SOCIAL MEDIA USE BY MOBILE TELEPHONE OPERATORS IN KENYA

Barack Ephraim Odhuno

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION, SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

OCTOBER, 2014

DECLARATION

Student's Declaration

This research project is my original work and has not been presented for a degree in this university or any other university.

Signature: --- Date: -----------------------------

Barack Ephraim Odhuno

D61/62672/2010

Supervisor's Declaration

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

Signature: --- Date: ---------------------------

James T. Kariuki

Lecturer

School of Business, University of Nairobi.

DEDICATION

This research project is dedicated to my parents, the late Charles Jacob Aura and Phoebe Okungu Aura who are my mentors and instilled in me at a tender age the value of a good education.

ACKNOWLEDGEMENT

I acknowledge the power of the Almighty God for having brought me this far. Indeed His calming whispers created an enduring spirit and determination that helped me to complete my studies.

I owe a lot of gratitude to my late father Mr. Charles Odhuno Aura whose love for education inspired me from a young age to aim to be the best that I could ever become in life. I also thank my mother whose life story has been a source of strength and encouragement as I undertook my studies. My wife Awuor has been a great source of love and support during the period of my studies, indeed I am greatly indebted to her.

I also remember my late Uncle Jerry Okungu who was my best friend. Indeed his insights in management and business will remain with me forever. My sister Julie cannot go unmentioned, she always found a way to make me relax and focus on my studies.

Last but not least, I remember Moses Aluodo, my cousin who created time to help me with the data collection. I cannot forget Mr. Rune Karlsen who has been my boss for the last 8 years. His belief in me to grow and become a manager will stay with me for the rest of my life.

Lastly, to Mr. J.T. Kariuki, for his patience and understanding of my work schedules, I am truly grateful and honored to have been your student.

To all my other lecturers especially Dr. Murang’a Njihia and Dr. Kate Litondo who kept demanding the best from me during my course work, God bless you all.

ABSTRACT

Mobile telephone operators in Kenya have been using social media in their business activities. The objectives of this study were to determine the extent to which social media is used by mobile operators in Kenya, to identify the risks that mobile operators are exposed to when they use social media and to determine the mitigation measures that they have put in place in order to mitigate the risks. A descriptive survey research design targeting managers in the Human Resource, Marketing, Customer Service, Operations, Legal, Social Media and Information Technology departments in the four mobile operators in Kenya was adopted at the time of the study. The study utilized primary data that was collected through a self-administered structured questionnaire. One of the key findings of the study was that social media had been widely adopted by the mobile telephone operators in Kenya. Secondly, the study established that mobile operators were exposed to social engineering attacks, disclosure of intellectual property rights, disclosure of confidential information, malware spread and non-compliance to privacy laws when they use social media. Lastly, the study established that mobile operators enforced social media policies, monitored activity on their social media sites, trained their employees and used symbols in risk communication to mitigate their exposure to social media risks. The study recommended that the mobile operators should adopt a training model that includes an annual or bi-annual refresher sessions for all employees in addition to the first social media training that is done when the employees are newly employed in order to increase the state of awareness of social media risks. The study also recommended that the mobile phone operators should adopt a co-ordinated and integrated approach to social media policy development. Lastly, mobile telephone operators who do not have disaster management plans should develop them in order to have a clear set of procedures to use in decision making in case of a social media breach or attack.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATIONS

BPO	Business Process Outsourcing
CDMA	Code Division Multiple Access
CV	Curriculum Vitae
E-Democracy	Electronic Democracy
E-Governance	Electronic Governance
FERF	Financial Executives Research Foundation
GSM	Global System for Mobile Communications
HR	Human Resource
ICT	Information and Communication Technology
IEBC	Independent Electoral and Boundaries Commission
IT	Information Technology
RSS	Really Simple Syndication
UK	United Kingdom

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

An individual's success in society depends on the shape and size of his or her social network and ability to network and form connections with other social groups (Zyl, 2008). Consequently, organizations which can harness this innate human ability to manage knowledge are able to lower transaction costs and become more profitable (Zyl, 2008). One of the ways of networking and forming connections with other social groups is through social media. BITS (2011), defines social media as any kind of online interaction that allows for a highly scalable publication of user generated content of any kind whether video, audio, text or images that is meant for general public consumption and uses interactive dialogue with others. On the other hand, Kanter (2010) refers to social media as an array of digital tools such as instant messages, blogs, videos and social networking sites such as facebook and MySpace that are inexpensive, easy to use and enable people to create, manipulate and share their own stories, videos and photos. Social media applications are driven by web 2.0 technologies. Web 2.0 technologies are the perceived second generation web-based platforms consisting of applications specifically designed to aid online collaboration and user generated content sharing (Clearswift 2007a; Matuzak, 2007; O'Reilly, 2005)

The use of the web 2.0 technologies has revolutionized communication over the internet. The integration of these technologies in social media sites has made them encourage user participation and interaction. Web content is therefore no longer merely examined but it is shared, critiqued and developed collaboratively (Petty, 2012). Over time, social media has crept also into the business domain (Zyl, 2008). More than one third of social media users have used it to praise or criticize a company, brand or product thus creating good opportunities for marketers to promote their brands, encourage customer participation in brand promotions as well as learn more about their customers (Burshtein and Turco 2010; Rein 2011). Apart from product marketing, social media has been credited with the ability to expand social contacts, accelerate business processes, improve customer relations, cost effective recruitment of high caliber of staff, improvement of staff morale, staff motivation and job satisfaction among staff (BITS, 2011).

1.1.1 Social media risks and risk mitigation measures

Thornton and FERF (2011) warn that, social media is the proverbial double edged sword that offers both opportunities and risks. Social media is especially attractive to online criminals because it is inherently viral by its nature (Symantec 2011). According to Zyl (2008), the fact that people can access a large amount of information on social media with ease makes its users vulnerable to social engineering attacks. Spammers and virus writers can set up false profiles and trawl through social networking sites including blogs gathering information about job titles, phone numbers, and email addresses (Message Labs, 2007a). Organizations also expose themselves to potential loss of confidential information, resource wastage with regards to server and network bandwidth as well as damage to organizational reputation through negative remarks from disgruntled employees and customers (Zyl, 2008).

To take full advantage of the benefits and opportunities presented by social media, organizations must develop risk mitigation measures to mitigate the risks involved its use. Thorton and FERF (2011) propose that organizations should develop a social media policy and integrate it with other company policies as well as align it to the organizations strategic direction. They further state that where a company might have an electronic communication policy to address appropriate uses of the company’s computer system, then the existing policy should be amended and updated to include aspects of social media. Additionally, because social media cuts across many areas of a company including HR, marketing, communications and legal among others policies surrounding it should be the result of a multidisciplinary approach (Thorton and FERF, 2011). To be effective, a social media policy must be part of a co-ordinated and properly documented human resource strategy (Chelia and Field, 2012). As the types of social media risks vary, so do the strategies of mitigating them and if employees and businesses are serious about managing social media, they must get serious about developing a human resource strategy that not only includes documented policies and procedures but also an internal training program and a robust record keeping procedures (Chelia and Field, 2012).

1.1.2 Social media in Kenya

Social media has mostly been viewed as a personal communication tool. From a personal user perspective, it is used as a means to communicate with friends and relatives in addition to existing communication or replacing existing communication methods has been monumental. According to Socialbakers (2013), there are 1,886,560 registered facebook users in Kenya and Kenya ranks sixth in Africa in terms of population usage of facebook. Furthermore, a report titled “How Africa Tweets” by Portland Communications and Tweetmister suggests that in the last quarter of 2011, Kenya posted 2,476,800 tweets making it the second most active country on the social networking site twitter. In Kenya, social media has been used by businesses to market their products and services, recruit employees and professional staff and even provide customer service. Because of the popularity of social media in Kenya, organizations including government agencies like the Independent Electoral and Boundaries Commission (IEBC) have realigned their location strategies to include social media so that they can tap into the endless opportunities. According to Socialbakers (2013), the top 5 brands that use facebook in Kenya are Safaricom Kenya Limited, Samsung Mobile

Kenya, OLX Kenya, Midcom East Africa and Airtel Kenya respectively while the top five Kenya Brands on Twitter are Safaricom Limited, Kenya Airways, Safaricom Customer Care, IEBC and Samsung Mobile Kenya. The most commonly used social media platforms in Kenya are Facebook, Twitter, You Tube, LinkedIn and Google+.

1.1.3 Mobile operators in Kenya

There are four mobile telephone operators in Kenya namely Safaricom, Airtel, Orange and Yumobile. Safaricom Limited is the leading mobile operator in Kenya with a subscriber base of over 19.1 million. Formed in 1997 as a fully owned subsidiary of Telkom Kenya, its ownership has mutated over the years. Vodafone, a United Kingdom (U.K.) based mobile telecommunication company owns 40%, the Kenyan Government owns 35% and the public shareholders own 25% of Safaricom. With an aim to becoming the best company in Africa, a strong focus has been placed on quality of service in order to gain competitive advantage over other industry players.

Airtel Kenya on the other hand was launched in Kenya in 2010 having started out as Kencell in 2000 and rebranded to Zain in 2008. With a subscriber base of 5.2 million, it is the second largest mobile operator in Kenya. It is owned by Bharti Telecom, an Indian based telecommunication service provider.

The Orange brand is a partnership between Telkom Kenya and France Telecom Group. Formed in 2008, it prides itself as being the only mobile operator in Kenya with an integrated services solution operating on both GSM and CDMA licenses. Its subscriber base is 2.7 million with countrywide presence on both GSM and CDMA platforms.

The fourth mobile operator in Kenya is Essar Telecom. Launched in 2008 under the brand Yumobile, it prides itself as the only mobile operator to have achieved countrywide coverage ten months from its launch. It has a subscriber base of 3.2 million and is owned by the Essar group which is a multinational conglomerate and is a leading player in sectors of steel, oil, gas, power, Business Process Outsourcing (BPO), telecom services, shipping, ports and projects. The Essar group has operations is in more than 25 countries across five continents employing more than 75,000 people and has revenues of over 27 billion dollars.

1.2 Statement of Research Problem

Social media has been adopted by Kenyans as an avenue for social networking, political participation and interactions among themselves as well as with other people around the world. Businesses have also realized the potential benefits and opportunities in its use and have adopted it as a strategy to achieve competitive advantage. Such benefits include improvement of customer relations, viral marketing, product and service recommendations and product development through customer feedback among many others. Inspite of the benefits and opportunities presented by social media, there are also risks associated with its use. Such risks include disclosure of intellectual property, disclosure of confidential information, decreased productivity, social engineering attacks, spreading of malware and non-compliance to privacy laws.

Studies on social media and social media risks have been undertaken both internationally and locally. Internationally, Petty (2012) examined the common risks posed by social media to brand marketers and concluded while that brand marketers have the opportunity to use social media as an inexpensive channel for brand promotion, they are faced with social media attacks and they need to monitor their brands on social media with an aim of addressing negative brand images that may be posted by brand imposters. Thorton and FERF (2011) studied social media and its associated risks on financial institutions in America and confirmed that social media offers both opportunities and risks. They also concluded that governance regarding social media was fragmented and each company had its own opinions about social media, its potential uses, risks and risk management strategies. The Ponemon Institute (2011) focused on social media risks for IT practitioners and recommended that there is a need to create and understanding of the risks social media tools create in the work place. Locally, Mwangi (2012) showed that Safaricom Ltd has used social media to improve its customer service while Chebet (2012) indicated that social media has been used by Safaricom Ltd as a strategic communication tool.

One of the industries in Kenya that has adopted social media is the mobile telephone industry. The four mobile telephone operators in Kenya are Safaricom, Airtel, Orange and Yumobile. To fully exploit the benefits and opportunities presented by social media, it is important for the mobile telephone operators to identify the risks involved in social media use and determine risk mitigation measures that may be employed to eliminate risks or reduce the impact of those risks.

The studies on social media that have been carried out on in Kenya so far have focused on the benefits and opportunities presented by the use of social media. Internationally however, studies prove that there are risks associated with social media use and that risk mitigation measures must be put in place to exploit the full benefits and opportunities presented by social media. This study therefore aimed to create an understanding of the management framework of social media in the mobile telephone operator firms in Kenya by determining the extent to which social media is used by mobile operators in Kenya, identifying the risks that mobile telephone operators face as they use social media and determining the risk mitigation measures employed by the mobile telephone operators in Kenya to mitigate the risks. Consequently, the questions that this study aimed to answer were: To what extent do the mobile operators use social media in Kenya? Secondly, what social media risks are mobile telephone operators in Kenya exposed to? Lastly, what are the social media risk mitigation measures that mobile operators in Kenya have put in place in order to mitigate social media risks?

1.3 Objectives of the Study

The objectives of the study were to:

1.) Determine the extent to which mobile telephone operators in Kenya use social media in business.

2.) Identify the risks associated with social media use by mobile telephone operators in Kenya.

3.) Establish the risk mitigation measures taken by the mobile telephone operators in Kenya to mitigate the risks in social media use.

1.4 The Significance of the Study

The findings of this study will be of great importance to stakeholders that use social media. First of all the recommendations from this study will help the mobile operators using social media to understand the gaps in their social media risk mitigation strategies and improve where they may fall short.

Secondly, through this study, other businesses intending to adopt social media will have an understanding of the potential benefits, risks and risk mitigation strategies thus enabling them to use social media in a manner that exploits the full benefits and opportunities provided by social media.

The government through its policy makers, regulatory and security agencies will also have a better understanding of social media risks and the risk mitigation strategies. This will then help them in the management of information posted on government social media sites and in the public at large.

The General Public also needs to understand social media and its use. Users upload photos, videos and a lot of personal information. The risks involved in such postings need to be identified and the public informed on how to mitigate their impact and manage personal profiles on social media.

The academia may also find the findings of this study useful in enhancing their knowledge about social media risks, mitigation measures and management in organizations.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter presents a literature review related to the use of social media in business enterprises, the risks associated with social media use and the social media risk mitigation measures. The review starts with an understanding of web 2.0 technologies and social media to establish a clear relationship between the two. A critical look at the benefits and opportunities of social media use in organizations then follows after which the possible risks of social media use in organizations are assessed. Risk mitigation measures finally conclude this chapter.

2.2 Social media

BITS (2011), defines social media as any form of online interaction that allows for a highly scalable publication of user generated content of any kind (test, audio, video, images) that is meant for general public consumption and uses interactive dialogue with others. It is differentiated from traditional online publication in that the communication tends to be more dynamic, personal and interactive (BITS, 2011). Wellman (2001) asserts that social media involves social relations amongst people who have some type of relationship or affiliation. According to Wasike (2012), it encompasses blogs, Wikis, MySpace, Facebook, RSS, Flickr, Tag, Cloud, Folksonomy, Twitter among others and that it may be conceptualized as socio-technical arrangements incorporating technologies that support such arrangements. Aula (2010) states that social media is characterized by interactivity where participants freely send, receive and process content for use by others and that its services include social networking, content production, distribution of services and websites that are collectively constructed by users (“wikis such as Wikipedia), video and photo sharing services such as (YouTube and

Flickr, virtual worlds (second life), and diary type websites ("blogs"). His corporate perspective of social media services includes facebook, music, entertainment focused MySpace, career oriented LinkedIn and network service twitter which lets members send out short messages via computer and mobile devices. Social media can therefore be defined as proposed by Kaplan and Heinlein (2010) as a group of internet based applications that build on the ideological and technological information of web 2.0 technologies to allow for the creation and exchange of user generated content. Web 2.0 technologies are the perceived second generation web-based platforms consisting of applications specifically designed to aid online collaboration and user generated content sharing (Clearswift, 2007a; Matuszak, 2007; O'Reilly, 2005).

In recent years, the ongoing development of internet technologies of social media and the increasing use of these tools have seen the web advance from a platform on information delivery to one that includes contribution and collaboration (Burford, 2012). Mc Afee (2009, P1) claims that valuable opportunities exist for organizations in the relocation of these technologies from open web to corporate intranets and uses the term "Enterprise 2.0 (the emergent use of software platforms in pursuit of organizational goals)" to describe internal hosting of web 2.0 technology and its use. Furthermore, according to Burford (2012), social media or web 2.0 technologies is increasingly used within organizations in pursuit of their informational and communicative goals and that in a similar vein to the initial web, web 2.0 exhibits emergent development and growth and has been adopted in a diverse range of forms and environments. She however cautions that while it is replete with novelty, innovation and potential, possibilities of failure and misuse also exist.

2.3 Benefits and opportunities in social media use in organizations

2.3.1 Introductions and recommendations of people

While analyzing the benefits of social media to organizations, Zyl (2008) starts by asserting that “It is not who you know but it is what who you know knows.” In organizations, knowledge comprises of experience, specialist skills and the practical knowledge of how the organizational processes operate (Orlikowski, 2002). According to Gorge (2007), social networking 2.0 provides users with the ability to create a global list of contact details (either in a graphical or text based format) of people with whom they have strong professional ties, co-workers, colleagues and people they do business with and who they trust enough to be associated with and even to recommend to others. The graphical expressions of personal relationships can be acquired over the span of an entire career, allowing users to identify mutual relationships which can be exploited for introductions or recommendations (Boyd, 2006; Gorge, 2007; Granovetter, 2004).

2.3.2 Knowledge sharing in organizations

Zyl (2008) notes that an important function of the office social system is the provision of a collaborative learning environment, in which problems encountered, are collectively solved and solutions shared among users thus bridging the gap between procedures and practice. According to Tapscott and Williams (2006), knowledge is increasingly viewed as a product of networked people that are looking for new solutions to specific problems. Zyl (2008) further states that knowledge and information typically spans across many types of communication tools, document formats, desktop applications and sources within and outside the firewall and can include email, faxes, instant messages, manual, spreadsheets and presentations. Social media by its nature of being collaborative therefore provides a good platform for knowledge to be shared within the organization. More importantly though, through social media, knowledge workers are able to aggregate information in an efficient manner by adding labels (through links, tags and social bookmarks) to make material more persistent for easy retrieval and sharing (Zyl, 2008).

2.3.3 Maintaining staff morale and job satisfaction

According to Zyl (2008), maintaining staff morale and job satisfaction, while maintaining discipline and productivity has become one of the biggest challenges to managers. On the other hand, Tapscott and Williams (2006) argued that the open platforms of social media take away the friction as a result of collaboration thus creating a culture of sharing and increasing job satisfaction.

Secondly, social media rewards contributions through ratings, feedback and the creation of a following from people who link to or subscribe to your work. This digital reputation serves to recognize a person's contribution to and beyond the immediate group and places value on the individual's knowledge and knowledge creation abilities (Brown and Duguid, 2000; IBM, 2007). This increased visibility satisfies most an individual's desire for prestige and recognition and increases their job satisfaction (IBM, 2007).

2.3.4 Improvement of customer relations

Social media platforms provide customers with a direct access to information for which they would previously have had to telephone or email (Zyl, 2008). This eliminates frustration caused by delays (Clearswift 2007b). The tools of social media shift the one-way communication model from a professional to client to a vibrant conversation. Relationship and engagement with clients is given opportunity by the potential of social media and practitioners attempt to develop an interaction with their audience that endures and requires ongoing commitment by community members (Burford, 2012).

2.3.5 Social media as a viral marketing tool

Through social media, people are encouraged to voluntarily pass marketing messages on through word of mouth (IBM, 2007). Zyl (2008) further notes that viral promotions may include video clips, flash games, e-books, free software, images and text books.

2.3.6 Innovation

Social media is a valuable and enabling intermediary for collecting societal knowledge (Burford, 2012). By monitoring customer communications, feedback and opinions, innovation can be encouraged (Matuszack, 2007; Tapscott and Williams, 2006). This continuous communication with customers can be used for solution development by utilizing customer opinions in making key product decisions (IBM, 2007).

2.3.7 Recruitment

In their white paper social networking, Security and your Business: A Guide for IT Managers, Symantec (2011) observes that a vibrant social network around a company can make it attractive to new recruits and even help new hires settle in more quickly. Similarly, it helps HR with recruitment and for many users and companies, LinkedIn is a kind of CV exchange and services such as BranchOut are bringing recruitment to facebook too.

2.4 Risks of social media use in organizations

Risk refers to potential problems that would threaten the success of a project. These potential problems might prevent a project from achieving its objectives by increasing time and cost, lowering the quality of project outputs or preventing the project from being completed all together.

Risks can occur at any stage in a project. Some are associated with particular tasks and others originate themselves from outside the project and can manifest themselves without warning. Generally speaking, a risk event that occurs late in a project can be more costly in terms of time and money than a similar event nearer the start of the project. This is because as time passes there will be greater value of work in progress and higher sunk costs of loss or damage.

While some small or similar projects might not need special attention to risk management, complex and large projects need a comprehensive risk management strategy to identify as many potential risks as possible and then decide how to deal with them. The following are as some of the risks organizations expose themselves to if they deploy and use social media within their organizations.

2.4.1 Risk of non-compliance to privacy laws

Privacy is the ability of an individual or group to choose the extent and circumstances under which his or her beliefs, behaviours, opinions and attitudes will be shared with or withheld from others (Duncan et al, 1993). The right to privacy is ones right to keep a domain around him or her including all the things that are part of them such as their bodies, homes, property, thoughts, feelings, secrets and identity (Onn et al,2005). Onn et al (2005) further suggest that the right to privacy gives one the ability to choose the parts of their domain that can be accessed by others, and to control the extent, manner and timing of the use of those parts they choose to disclose. The right not to be subjected to unsanctioned invasion of privacy by government, corporations or individuals is part of many countries' privacy laws and in some cases, constitutions. In Kenya for example, the right to privacy is spelt out in the Kenyan constitution under article 31 which states that every person has a right to privacy which includes the right not to have their person, home or property searched, their possessions seized, information relating to their family or private affairs unnecessarily required or revealed and the privacy of their communities infringed. Further article 35, sub-article 2 states that every person has the right to the correction or deletion of untrue or misleading information that affects the person. Additionally, the Constitutional Implementation Commission of Kenya has been working on the Access to Information and Data Protection Bill which clearly spells out all the privacy rules to abide by in Kenya. Following the Presidential Speech on the 16th of April, this will hopefully become law as it will be proposed to parliament for debate. Therefore regardless of how companies and individuals perceive privacy, companies need to understand the privacy and protection laws, including those in countries in which they do business (BITS, 2011). With the increasing volume and depth of personal information available online come increasing risks to privacy (BITS, 2011). For organizations operating multinationally, the high number of laws and regulations related to privacy and the rights to privacy pose challenges to the adoption of information based services such as social media thus forcing them to weigh regulatory and legal obligations against their wish to serve their customers and meet business goals and this balancing act poses a great challenge given that the primary purpose of social networking is a broad disclosure of information including individual’s personal information (BITS, 2011).

Apart from the regulatory and legal requirements, social media sites are granted authorities such as perpetual licenses to provided information and so while an organizations use of collected information may align with the stated privacy practices, the social media provider’s use may not (BITS,2011). At the same time, customer communications operate under a social media site’s rules and not those of the organization.

The challenges of the delicate balancing act to be in line with the legal and regulatory framework as well as the lack or real ownership of a social media site therefore puts an organization at a great risk of unknowingly not complying with the privacy laws or invading the privacy of its employees or customers and is a potential subject of litigation (BITS, 2011).

2.4.2 Identity theft

While social networks like facebook are a great way to share information that is important to an individual, they are also fertile ground for criminals looking for information such as full date of birth, home addresses and other personal information used to commit identity theft (BITS, 2011). Identity theft is a crime in which an imposter obtains key pieces of personal information such as driver's license numbers or social security numbers in order to impersonate someone else and use the information to obtain credit, merchandise and services in the name of the victim or to provide the thief with false credentials (Laudon et al, 2010).

Most authentication methods in use today include the use of shared secrets which is generally comprised of information available from public records as well as out of wallet information such as the name of the oldest nephew, date of birth, name of poet e.t.c. In many cases, this information is shared in posts, photos and profiles published on social media sites. The user's ability or inability to control access to this information posted on the social media sites has been a source of controversy. According to Vander Veer (2008), 25% of social media users cannot find security settings provided by social media sites leaving them at the mercy of the default settings on these sites. The lack of transparency on the social media service provider on what information is being shared and with whom, a lack of user controls to provision access to their posts, as well as misconfigured privacy settings can all expose users to unintentional sharing of personal or confidential employee and corporate credentials which may enable hackers to obtain answers to standard security challenge questions (BITS, 2011). For example, corporate profiles and information shared or contained within an employee's personal or professional profile may provide tips for guessing ids or passwords for access into corporations' internal applications or systems.

2.4.3 Spreading malware

Malware, short for malicious software, is software designed to harm a computer system without owners consent or knowledge by exploiting existing vulnerabilities and flaws in computer software that create weaknesses in systems making their entry easy and discreet (Laudon et al, 2010) . The software includes viruses, worms and Trojan horses. Ponemon Institute (2011) established through survey done on 4640 IT and IT Security practitioners in Canada, United States, France, Germany Italy, Australia, Singapore, Hong Kong, India, Brazil and Mexico, that viruses and malware infections are on the rise on social networks. Another report published by Symantec (2011) indicates that malware is on the rise on social networks such as Facebook, Twitter, LinkedIn and MySpace. In this report, 36% of the 500 respondents reported being sent malware via social networking sites and this was an increase of 70% from the previous year. 65% of the respondents stated that facebook was the biggest security risk, followed by MySpace, Twitter and LinkedIn.

Malware spread through social networks into the institutions infrastructure and data comes through employee use of social networks or through remote devices. Such attacks could easily threaten consumers' trust in the institutions' security measures and handling of their personal information (BITS, 2011).

2.4.4 Social engineering attacks

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information, namely the unauthorized acquisition of sensitive information or inappropriate access privileges by a potential threat source (BITS, 2011). The term typically applies to exploitation of trust or building of an inappropriate trust relationship with a legitimate user, the creation or exploitation of confidence or vanity to gather information or influence the actions of another individual or entity for information gathering or computer system access (BITS, 2011). Its goal is to trick someone to divulge information that they would otherwise not share or divulge through techniques such as pretexting, phishing, pharming and phonephishing (BITS, 2011). Social engineering is proliferating and evolving so rapidly that standard security policy, operational procedures and technical solutions cannot adequately protect institutions (BITS, 2011).

2.4.5 Disclosure of intellectual property and confidential information

Users of social media can advertently or inadvertently share information that is considered sensitive or proprietary from a business perspective FERF and Thorton (2011). The risk here entails accidental or intentional disclosure of company secrets, strategies or other proprietary and possibly patented information via social media sites as well as private information about clients or other outside users and stakeholders FERF and Thorton (2011). A company can therefore be put at risk of civil legal action surrounding the failure to protect such data, regulatory penalties and even loss of reputation and damaged brand (BITS, 2011).

2.4.6 Lack of productivity

One of the biggest concerns regarding social networking platforms is that productivity will be affected negatively because employees may spend too much time networking and posting entries on blogs and wikis (Zyl, 2008). There is also a risk that employees will utilize it for more special purposes and not on work related postings (Ariyur, 2008; Clearswift, 2007b; Messagelabs, 2007a). This can have serious implications with regards to the capacity and utilization of servers and networks, with bandwidth being congested with multimedia contents which are often not work related (Clearswift,2007d; MessageLabs,2007a). The challenge for companies is to find a way to preserve workforce productivity by limiting access to social media applications without restricting workers access to business benefits (Cisco, 2012).

2.4.7 Misinformation

In social networking, knowledge is no longer created in controlled hierarchical groups and user generated information created using collaboration tools such as blogs and wikis, allow anybody to add and edit content, including unanticipated players who are not subject matter experts (Ariyur,2008;ClearSwift,2007b). This peer produced knowledge may not be as reliable as procedures and manuals generated by specialist staff and communicated down the chain of command and might be a big source of misinformation internally. Externally, vandalism and misinformation caused by employees can leave employers open to legal action (under the principle of vicarious liability), whereby employers are responsible for neglect acts or omissions by their employees in the course of their work, even if those acts are accidental (ClearSwift, 2007c).

2.4.8 Reputation risk

Aula (2010) defines reputation risk as the possibility or danger of losing one’s reputations. He asserts that the loss of reputation affects competitiveness, local positioning, the trust and loyalty of stakeholders, media relations, legitimacy of operations and even the license to exist. He further argues that social media expands the spectrum of reputation risks and boosts risk dynamics through users who generate unverified information which are both true and false. According to him, both true and false ideas, put forth in social media sites can differ greatly with what is true about the organizations and from what the organizations share with the public.

Damage to organizational reputation can be caused by articles appearing in the press about employees being dismissed by an organization for inappropriate use of office resources (Netconsent Limited, 2004). Former and dissatisfied customers can also criticize and complain about the organization creating a public image outside the organization’s control (Shirky, 2008). Unethical and illegal web content from untrustworthy information sources containing factual inaccuracies and errors transmitted especially to a third party social media sites could also cause irreparable damage to a company’s reputation (Rudman, 2009).

2.5 Social media risk management and mitigation measures

Risk management is the evaluation of potential risks and development of strategies to reduce the risks and learn about future risks. It involves risk identification including probabilities and impact, identification of possible solutions to the risks, implementation of the solutions and risk monitoring to learn future risk assessment (Chaffey D and Wood S, 2005).

The rise of social media should not be considered isolated or unique but rather an evolution of online communications with special considerations when used in a very broad and public setting and whose control requirements may not be unique but may be challenged given the ways technologies are deployed (BITS, 2010). For many companies, social media is the proverbial double edged swords offering opportunities and risks cutting across many areas of the company including HR, marketing, communications, legal among others and while no one can foresee all the risks, they must be anticipated in order to be properly addressed (FERF and Thornton,2011). Social media risks can be mitigated in the following ways.

2.5.1 Monitoring

To effectively use and manage social media, a company needs to closely monitor posts, tweets or even comments regarding the firm, brand, executives and associates whether they are positive or negative. Petty (2012) points out that monitoring may reveal negative social media postings by employees and many organizations are adopting social media policies for employees that include prohibition of disparaging remarks even if posted from home computers after work hours. She further proposes that apart from identifying disgruntled employees, monitoring can be used to find people who are pretending to be disgruntled employees or others who are simply not clear about their relationship to the company but whose comments are disparaging and reputation damaging. In addition to monitoring for disparaging remarks, she asserts that social media marketers have an obligation to tell network members what is and what is not factually accurate about the product to prevent them from making deceptive or unsubstantiated claims. Finally she cautions that because network marketers cannot monitor every single blog or statement, organizations need to have a system in place to monitor information and not let misleading claims go out of control. According to Rein (2011) one way of ensuring this is to subscribe to the services of one or more brand protection internet security firms. Other parts of such a monitoring system could include a well scoped monitoring plan with a clear and prioritized response plan and escalation contacts for negative or harmful postings from both external and internal sources as proposed by BITS in their Financial Services Round Table Report of 2011. According to this report, organizations must have various social media monitoring tools that match with their social media strategy.

2.5.2 Risk communication

According to Pattinson and Anderson (2007), the manner in which people see risks associated with information security determines what decisions they will make regarding the actions they will take (or not take) in conjunction with whatever security measures their organization has put in place. They outline that one of the factors purported to have an influence on risk perception is the way in which a risk message is communicated to computer end users and management. Bener (2000) claims that the manner in which risk is communicated within an organization substantially influences the risk perception of the different individuals within that organization. Lipa (1994) voiced the same opinion that an individual's perception of risks is shaped by the way in which risky situations are communicated to them within a particular context.

Pattinson and Anderson (2007), identify security awareness seminars, standard email memos, notice board memos, phone calls, web pages, one on one discussions, group meetings and flyers as some common forms of risk communication. However, they propose that together with these information security messages, symbols and graphics would improve the effectiveness of risk communication in the organization and the general perception of the risks to the information systems would be more realistic.

2.5.3 Training

A report from BITS (2011) enumerates training employees on social media use, risks, company policies and guidelines as the first line of defence for preventing in-appropriate dissemination of content by employees and for sensitizing them to potential reputational risks from outside sources. It proposes that the content of the training programme should include who is permitted to use social media and the standard for gaining access, what social media tools are permitted by the company, which ones are forbidden, how the tools work and what is their potential impact on the company's reputation, all the company guidelines for the frequency, style, tone and length of content, all relevant corporate policies on the code of conduct pertaining to external communications, the review process for content before it is posted publicly, the escalation process when it is appropriate to activate and the consequences of inappropriate or unauthorized use of social media.

Further they suggest that the model of training should be upon hiring and repeating annually or semi-annually.

2.5.4 Social media management framework in the organization

FERF and Thornton (2011) argue that employers should approach social media and social networking tools from a social media policy perspective for its effective and efficient management. The same argument is fronted by BITS (2011) that a clearly posted and well communicated social media policy around the usage of social media on and off network is one of the most important risk mitigation measures. Chellia and Field (2012) link social media policy and the employees' contracts in risk mitigation by reiterating that an employer's position could be strengthened by having a clearly defined internal grievance procedure as well as a well-defined policy on the use of social media that refers back to the employment contract and stresses that posting negative comments about the organization and work colleagues is not acceptable.

FERF and Thornton (2011) however caution that because social media cuts across many areas of a company like marketing, HR, legal, communications among others, any policy surrounding it must be the result of a multidisciplinary approach. Chellia and Field (2012) detail this further by stating that if employers are serious about managing social media risks in their organizations then they must get serious about developing a well co-ordinated human resource management strategy that not only includes documented policies and procedures but also an internal training program and robust record keeping procedures. In addition to an all inclusive approach stated above, BITS (2011) encourage companies to develop policies that are narrowly tailored and not overly broad. The policies must balance the employer's needs to protect themselves and the employee's right to a personal existence and voice as well as reference other related policies such as code of ethics, internet usage, info security, prohibition on disclosure of employer’s confidential information, trade secret information as well as proprietary information. Finally they advise that the policies must contain clear statements concerning the employee risks if they do not adhere to the policies, intent to monitor employees and the fact that employees should have no expectation of privacy when engaging in activities on social media on and off network.

There are however instances where a company might not need a new social media policy. FERF and Thorton (2011) argue that in cases where another policy covers aspects of social media, that policy could be amended and updated instead of preparing another social media policy. For example, an electronic communication policy could be amended to address the issues of social media.

2.5.5 Response plan in times of policy breaches

Having a plan in place for dealing with instances of fraud and or privacy breaches related to social media is crucial should a company ever find itself a victim of either (FERF or Thornton, 2011). Discipline and termination procedures to ensure that when a social media event occurs, management is well versed to manage the situation fairly must also be put in place (Chelia and Field, 2012).

The viral nature of communications through social media means that a company’s reputation can be instantly heightened or damaged with a hit of the <enter key> (BITS, 2011). According to them, the most effective crisis planning and response involves an integrated effort among key parts of the company, including but not limited to, corporate communications, marketing, legal, information technology and human resources. Further, they assert that an effective plan should first of all have clear criteria for identifying risks that are likely to develop into a crisis. Secondly, a clear escalation process that details the next steps in addressing the crisis must be developed. Lastly, organizations must have a robustpre-crisis preparation, detailed responses for different kinds of crisis and a process for evaluating the success of the crisis.

2.6 Summary

The literature review for this study provided an understanding of social media, its potential benefits and opportunities, the risks a business may expose itself to while using social media as well as the mitigation measures that may be employed to mitigate the impact of the risks. Some of the potential benefits of social media are marketing of products and services, recommendation of products and services to potential customers, product development and innovation through customer feedback, maintaining of employee satisfaction and staff morale and knowledge sharing within the organization. On the other hand, some of the risks an organization using social media may expose itself to include spreading of malware, disclosure of confidential information, disclosure of intellectual property, non-compliance to privacy laws, reduced productivity, misinformation to customers and social engineering attacks. Lastly, some of the social media risk mitigation measures that an organization may employ include enforcing the social media policy, activity monitoring on social media sites, training and risk communication using symbols. This study aimed to create an understanding of the management framework of social media in the mobile telephone operator firms in Kenya by determining the extent to which social media was used by mobile operators in Kenya, identifying the risks that mobile telephone operators faced as they used social media and determining the risk mitigation measures employed by the mobile telephone operators in Kenya to mitigate the risks.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter describes the methodology that was used to carry out the study. It contains the research design, the target population, the data collection and data analysis methods that were used to conduct the study

3.2 Research Design

The study was undertaken using a descriptive survey research design. A descriptive survey research methodology was appropriate because the study aimed to describe social media use and management in the mobile telephone industry in Kenya by determining the extent to which it is used by the mobile telephone operators, identifying the risks encountered in its use and establishing the mitigation measures that are employed to reduce the impact of exposure to the risks.

3.3 Target Population

The target population was the four mobile telephone operators in Kenya, namely Safaricom Ltd, Airtel Kenya, Orange Kenya and Yumobile Kenya. The need for a coordinated and integrated management approach in social media management made it important to collect data from different departmental managers in each organization. The departmental heads of Marketing, Human Resource, Customer Care, Information Technology (IT), Operations and Social Media in each of the four mobile telephone operators in Kenya were therefore identified as respondents to provide the data required. In total, the data for study was provided by 28 managers. Given that the number of managers targeted was small, a census approach of studying the population was adopted.

3.4 Data Collection

The study utilized primary data that was collected through a self-administered structured questionnaire. The questionnaire was divided into four sections. Section A collected the background information of the organization as well as the details of the person from whom the data was collected. Section B provided data related to the extent to which social media is used in the organization while the section C collected data related to the risks associated with social media in the organization. Section D focused on social media risk mitigation measures.

3.5 Data Analysis

The raw data collected from the respondents was systematically organized, coded and entered into a computer for analysis. The Statistical Package for Social Sciences Software (SPSS) was used to analyze the data.

The data obtained from section A was tabulated to provide the number of respondents and the corresponding number of years of work experience for those respondents.

The data collected from section B was used to determine the extent to which social media was used in the mobile operator firms. The likert scale used in the questionnaire helped to measure the perception of the respondents regarding the extent to which social media is used in their organizations. The frequency for each response was multiplied by the likert value allocated and divided by the number of responses received to determine the mean. The mean was then expressed as a percentage of the total possible likert scale value. The computed percentages were then used to determine the extent to which mobile telephone operators use each social media platform, the extent to which mobile operators apply social media to undertake business functions and the extent to which they benefit from using social media. The percentages further provided an indication of which was the most widely used social media platform, which business activity employed social media the most and which was the greatest benefit that the mobile operators drew from the use of social media.

Data obtained from section C aimed to identify the state of awareness of social media risks and the risks involved in social media use by the mobile telephone operators. The likert scale was once more employed to measure the state of awareness and the risk levels of different risks as perceived by the respondents. Once again, the frequency for each response was multiplied by the likert value allocated and divided by the number of responses received to determine the mean. The mean was then expressed as a percentage of the total possible likert scale value. This computed percentage indicated the respondents' state of awareness of social media risks and what was considered as the highest social media risk.

In section D, for questions 6 and 7, means and percentages were computed based on the likert scale values allocated and the frequencies of each response thus providing information on the risk mitigation measures employed by the mobile operators in Kenya, the extent to which they use the risk mitigation measures and the effectiveness of each risk mitigation measure. Content analysis was used to analyze the responses from questions 7-13 of section D in the questionnaire.

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION AND DISCUSSION

4.1 Introduction

This chapter presents an analysis of the data and discussion of the results. The data was analyzed using means, frequencies and percentages.

4.2 Response Rate

Out of the 28 questionnaires administered, 26 were filled and returned resulting into a response rate of 92.9%. This response rate was considered acceptable for data analysis.

4.3 Respondents Work Experience

Table 4.1 Distribution of Respondents by Work Experience

Years of Experience in the Company	Number of Respondents	Percent (%)
1	4	15%
2	7	27%
3	6	23%
4	3	11%
5 and Above	6	23%

Source: Survey Data

From Table 4.1, 57% of the respondents had work experience of 3 years and above. The heads of department therefore had sufficient information to provide data related to the objectives of this study.

4.4 Social media use in the mobile industry

Table 4. 2 Extent of use of social media platforms

Social Media Platform Used	No Extent at All	Low Extent	Average Extent	Great Extent	Very Great Extent	Mean extent of use	% Extent of Use
Facebook	7.7%	19.2%	11.5%	30.8%	30.8%	3.5769	71.54%
LinkedIn	3.8%	7.7%	38.5%	19.2%	30.8%	3.6538	73.08%
Twitter	23%	0%	30.7%	26.9%	19.2%	3.1923	63.85%
YouTube	19.2%	11.5%	19.2%	34.6%	15.4%	3.1538	63.08%
Internal Enterprise 2.0 Solution	11.5%	11.5%	30.8%	23.1%	23.1%	3.35	66.92%

Source: Survey Data

From table 4.2, 92.3% of the respondents indicated that they used facebook, 96.2% indicated that they used LinkedIn, 76.8% indicated that they used Twitter, 80.8% indicated that they used YouTube and 88.5% indicated that they used the internal enterprise 2.0 solution. The high number of respondents that use social media platforms indicated that social media has been widely adopted by the mobile operators in Kenya. In terms of extent of use of social media platforms, LinkedIn is used to the greatest extent within the organizations in the mobile industry at 73.08% extent of use followed closely by facebook at 71.54%. The least used social media platform is YouTube at 63.08% extent of use.

Table 4. 3 Extent of Social Media Application in the Organization

Social Media Application	No Extent at All	Low Extent	Average Extent	Great Extent	Very Great Extent	Mean Extent of Application	% Extent of Application
Customer service platform	0%	15.4%	30.8%	26.9%	26.9%	3.6538	73.08%
Communication of information to customers	0%	7.7%	19.2%	46.2%	26.9%	3.9231	78.46%
Communication of information to employees	15.4%	30.8%	23.1%	15.4%	15.4%	2.8462	53.60%
Marketing of products and Services	0%	3.8%	26.9%	38.5%	30.8%	3.9615	79.23%
Knowledge sharing among employees	11.5%	42.3%	30.8%	7.7%	7.7%	2.5769	51.54%
Personal use by employees	19.2%	3.9%	34.6%	26.9%	15.4%	3.1538	63.08%

Source: Survey Data

Table 4.3 presents the findings on how the mobile telephone operators apply social media in their organizations and the extent to which they apply it.100% of the respondents indicated that social media is used in their organizations to perform customer service, market products and services and communicate information to customers. A further 84.6% of the respondents indicated that they use it to communicate information to employees while 88.5% and 80.8% indicated that it is used for knowledge sharing and for personal use by employees respectively. With regards to the extent of social media application, it is used to the greatest extent to market products and services at 79.23% extent of use. It is also used to communicate information to customers and to offer customer service to an extent of 78.46% and 73.08% respectively. The findings therefore imply that the application of social media is used to a greater extent on organizational activities that are directly related to their customers than those that are directly related to their employees.

4.5 Benefits of social media use

Table 4.4 Extent of social media benefits

Benefits of Social Media	No Extent at All	Low Extent	Average Extent	Great Extent	Very Great Extent	Mean Extent of Benefit	% Extent of Benefit
Referrals and Introductions to Potential Customers	0%	50.0%	15.4%	15.4%	19.2%	3.0385	60.77%
Recommendations of Products and Services to Potential Customers	11.5%	7.7%	38.5%	15.4%	26.9%	3.3846	67.69%
Recommendations of Potential Employees	3.8%	38.5%	26.9%	19.2%	11.5%	2.9615	59.23%
Knowledge Sharing within the Organization	0%	38.5%	26.9%	23.1%	11.5%	3.0769	61.54%
Maintaining Staff Morale and Job Satisfaction	19.2%	50.0%	23.1%	0%	7.7%	2.2692	45.38%
Improvement of Customer Relations through Customer Feedback	0%	15.4%	30.8%	30.8%	23.1%	3.6154	72.31%
Viral Marketing	3.8%	3.9%	30.8%	30.8%	30.8%	3.8077	76.15%
Development of Innovative Products through Customer Feedback	0%	23.1%	19.2%	38.5%	19.2%	3.5385	71.85%

Source: Survey Data

The respondents’ perceptions about to what extent the mobile operators benefit from social media are presented by Table 4.4. 100% of the respondents agreed that mobile telephone operators have got referrals to potential customers, shared knowledge within their organizations, improved customer relations and developed innovative products through customer feedback as a result of using social media. 96.2% of the respondents acknowledged that that the mobile operators have done viral marketing and have had employees recommended to them through social media. Lastly, 88.5% and 80.8% of the respondents indicated that mobile operators have had their products and services recommended to potential customers and their employees' morale maintained respectively.

Further, the respondents indicated that viral marketing is the greatest benefit of social media use in the mobile industry at 76.15% followed by improvement of customer relations at 72.31% and development of innovative products through customer feedback at 71.85%. Maintaining staff morale and job satisfaction is a benefit albeit to a low extent with a percentage extent of benefit of 48.97%.

4.6 Social media risk awareness, risks and mitigation measures

4.6.1 Social media risk awareness

Table 4. 5 Risk awareness

State of Awareness	**Awareness Level (X)**	**Number of Respondents (F)**	**F(X)**	**Percent (%)**
Not Aware	1	0	0	0%
Low Awareness	2	7	14	27%
Average Awareness	3	12	36	46%
High Awareness	4	5	20	19%
Very High Awareness	5	2	10	8%
Mean State of Awareness ∑F(X)/∑F	**3.07**			**61.4%**

Source: Survey Data

From the findings presented in Table 4.5, 46% of the respondents indicated that employees within their organizations are moderately aware of social media risks with 27% of the respondents indicating that employees in their organizations are aware of social media risks. 19% and 8% indicated that employees in their organizations are highly and very highly aware respectively with none of the respondents indicating unawareness of social media risk awareness in their organizations. The mean state of awareness for all the four mobile operators in Kenya was 61.4% indicating a moderate state of awareness of social media risks by employees in the mobile industry in Kenya.

4.6.2 Social media risks

Table 4. 6 Social media risks and extent of risk to the organization

Social Media Risks	No Risk At All	Low Risk	Moderate Risk	High Risk	Very High Risk	Mean Risk Level	% Extent of Risk
Risks of Non-Compliance to Privacy Laws in Kenya	42.3%	15.4%	30.8%	11.5%	0%	2.115	42.31%
Identity Theft	15.4%	26.9%	42.3%	7.7%	7.7%	2.654	53.08%
Social Engineering Attacks	15.4%	15.4%	26.9%	38.5%	38.5%	3.000	60.00%
Spreading of Malware	11.5%	57.7%	15.4%	15.4%	0%	2.346	46.92%
Disclosure of Intellectual Property	15.4%	34.6%	26.9%	15.4%	7.7%	2.654	53.08%
Disclosure of Confidential Information	7.7%	30.8%	34.6%	26.9%	0%	2.808	56.15%
Reduced Productivity	3.8%	42.3%	46.2%	3.8%	3.8%	2.615	52.31%
Misinformation to Customers and	23.1%	19.2%	42.3%	15.4%	0%	2.500	50.00%

Source: Survey Data

The findings presented in Table 4.5 indicate that 57.7% of the respondents perceive non-compliance to privacy laws by mobile operators as a social media risk. A further 84.6% of the respondents agree that mobile operators are exposed to risks of identity theft, social engineering attacks and disclosure of intellectual property while 92.3% and 96.2% of the respondents indicated that mobile operators risk having their confidential information disclosed and the productivity of their employees reduced respectively. According to 76.9% of the respondents, there is a risk of misinforming customers and other stake holders when using social media.

On the level of risks, the respondents considered social engineering attacks, disclosure of confidential information, identity theft, and disclosure of intellectual property and reduced productivity from employees as moderate risks while spreading of malware and non compliance to privacy laws were considered as low risks.

4.6.3 Risk mitigation measures

Table 4. 7 Risk mitigation measures

Risk Mitigation Measures	No Extent at All	Low Extent	Average Extent	Great Extent	Very Great Extent	Mean Exten t of Use	% Extent Of Mitigation Measure Use
Training	3.8%	50.0%	11.5%	15.4%	19.2%	2.961	59.23%
Activity Monitoring on Social Media Sites	0%	7.7%	53.8%	19.2%	19.2%	3.500	70.00%
Use of Symbols in Risk Communication to Staff and Customers	7.7%	26.9%	34.6%	26.9%	3.8%	2.923	58.46%
Enforcement of Social Media Policy	0%	3.8%	30.8%	42.3%	23.1%	3.846	76.92%
Development of a Social Media Disaster Management Plan	42.3%	3.9%	30.8%	15.4%	7.7%	2.423	48.46%

Source: Survey Data

Table 4.7 presents the social media risk mitigation measures employed by the mobile operators and the extent to which they use the risk mitigation measures. All the four mobile operators had put in place risk mitigation measures to minimize their exposure to social media risks. 100% of the respondents indicated that their organizations used activity monitoring and enforcement of the social media policy as risk mitigation measures. A further 96.2% and 92.3% of the respondents indicated that their organizations trained their employees on social media and used symbols to communicate social media risks to their staff respectively. Lastly, 57% of the respondents indicated that their organizations had put in place a disaster management plan to be followed in case of a breach or attack.

On the extent of using the risk mitigation measures, training and use of symbols in risk communication to staff and customers were used to a moderate extent while development of a social media disaster management plan was used to a low extent. Enforcement of the social media policy and activity monitoring were used to a great extent.

4.6.4 Effectiveness of risk mitigation measures

The study sought to determine the effectiveness of social media risk mitigation measures.

Table 4.8 presents the findings.

Table 4. 8 Effectiveness of risk mitigation measures

Risk Mitigation Measure	Not Effective	Barely Effective	Averagely Effective	Very Effective	Extremely Effective	Mean Extent	% Extent of Effectiveness
Training	0%	38.5%	23.1%	15.4%	23.1%	3.2308	64.62%
Activity Monitoring on Social Media Sites	0%	7.7%	42.3%	30.8%	19.2%	3.6154	72.31%
Use of Symbols in Risk Communication to Staff and Customers	11.5%	11.5%	23.1%	38.5%	15.4%	3.3462	66.92%
Enforcement of Social Media Policy	0%	26.9%	23.1%	26.9%	23.1%	3.4615	69.23%
Development of a Social Media Disaster Management Plan	42.3%	7.7%	3.85%	11.5%	0%	2.1923	43.85%

Source: Survey Data

From the findings, the respondents indicated that enforcement of the social media policy, use of symbols in risk communication to staff and customers and training were moderately effective in social media risk mitigation while the social media disaster management plan was least effective. Activity monitoring on social media sites was identified as the most effective risk mitigation measure. It is also noteworthy that activity monitoring and enforcement of the social media policy were the risk mitigation measures used to the greatest extent and at the same time risk mitigation measures perceived by the respondents as the most effective.

4.7 Training on social media

Table 4. 9 Training on social media

Frequency of Conducting Social Media Training.	**Frequency**	**Percent (%)**
When Newly Employed	18	69.0
Annually	5	19.0
Bi-Annually	3	12.0
Other	0	0
Total	26	100.0

Source: Survey Data

Table 4.9 shows the frequency of training employees on social media in the mobile operator firms. 69% of the managers indicated that training on social media was done when the employees in their organizations are newly employed while 19% and 12% indicated that training was done annually and bi-annually respectively.

The training content for social media use in organizations covers a wide range of topics including but not limited to who is permitted to use social media, standards for gaining access, what social media tools are permitted by the company, which ones are not permitted, all relevant corporate policies on the code of conduct pertaining to internal and external communications and the consequences of inappropriate use of social media. Social media is also dynamic and undergoes changes in its nature from time to time. As a result, training content may need to be modified after a certain period of time. Consequently, organizations using social media should develop training models that train employees upon hiring and include refresher sessions either annually or bi-annually.

4.8 Responsibility of social media policy development

Table 4. 10 Social media policy development

Department	**Frequency**	**Percent (%)**
HR	3	11.5
Legal	5	19.2
Social Media Department	1	3.8
Marketing	9	34.6
All the above through a Co-ordinated Approach	8	30.8
Other	0	0
Total	**26**	**100.0**

Source: Survey Data

The findings as shown by table 4.10 indicate that according to 34.6% of the respondents the responsibility for social media policy development lay with the marketing department. 30.8% indicated it lay with all the departments through a co-ordinated approach to its development, 19.2% indicated it lay with the legal department while 11.5% indicated that the HR department was responsible for social media policy development.

The indication by a majority of the respondents that the marketing department was responsible for the development of the social media policy may be explained by the fact that the greatest use of social media by the mobile telephone operators revolved around marketing activities which are obviously performed by the marketing department. However, according to the literature review because a social media policy cuts across all the departments in an organization and because of the need to maintain a balance between the employers' needs to mitigate social media risks and protect themselves through policies and employees' rights to personal existence and opinions, a well co-ordinated multi-disciplinary, consultative and participative approach is recommended to develop a social media policy in organizations. Therefore, mobile telephone operators in Kenya who have not adopted an interdepartmental co-ordinated approach in developing their social media policies should adopt it.

4.9 Social media policy enforcement

Table 4.11 Responsibility of enforcing social media policy

Department	Frequency	Percent (%)
HR	7	26.9
Legal	3	11.5
Social Media Department	8	30.8
Marketing	8	30.8
Other	0	0
Total	**26**	**100.0**

Source: Survey Data

As shown by Table 4.11, 30.8% of the managers responded that social media policy enforcement lay with the marketing and another 30.8% indicated that it lay with the social media departments.

From the literature review, organizations need to have an internal grievance procedure and a well-defined social media policy that refers back to the employment contract and stresses that posting negative comments about the organization and work colleagues is prohibited in order to strengthen their position in mitigating social media risks. Further, social media policies should be well documented and should be included as part of an organizations training programme. Other departments involved in risk mitigation who undertake activity monitoring and risk communications are also directly involved in social media enforcement by way of their roles in the organization. Therefore to successfully enforce the social media policy a co-ordinated and integrated approach that cuts across all the departments in the organization should be adopted by the mobile operators using social media.

4.10 Social media disaster management plan

Table 4.12 Social media disaster management plan

Presence of a Social Media Disaster Management Plan	Frequency	Percent (%)
Yes	13	50.0
No	13	50.0
Total	**26**	**100.0**

Source: Survey Data

Table 4.12 indicates whether the mobile operator firms in Kenya have a social media disaster management plan or not. The study revealed that only half of the mobile telephone operators in Kenya have social media disaster management plans. This may explain why close to 43% of the respondents indicated that they do not perceive the disaster management plan as an effective risk mitigation measure. The impact of an attack on social media could damage the reputation of an organization because of its viral nature. Therefore, it is important for organizations to have clear procedures and action plans in cases of attacks or policy breaches in order to help them reduce the impact of the breaches or attacks when they occur.

4.11 State of preparedness in case of a security breach or attack

Table 4.13 State of preparedness in case of a breach or attack

State of Preparedness	Frequency	Percent (%)
Not Prepared	1	3.8
Ill Prepared	4	15.4
Averagely Prepared	15	57.7
Highly Prepared	4	15.4
Very Highly Prepared	2	7.7
Total	**26**	**100.0**

Source: Survey Data

The findings of the study with regards to the state of preparedness of the respondents in case of a social media security breach or attack are presented in Table 4.13. The study revealed that 57.7% of the employees in the mobile telephone operator firms were averagely prepared in case of a breach or attack through a social media platform. 15.4% of the respondents indicated the employees in their organizations were highly prepared while another 15.4% indicated they were ill prepared. A further 7.7% indicated their employees are very highly prepared while 3.8% are not prepared. With only 23.1% of the respondents indicating a high state of employee preparedness in cases of a social media attack in their organizations, mobile operators in Kenya need to take effective and efficient measures to ensure a high level of preparedness and reduction of the impact of social media attacks when they occur.

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter provides the summary of the findings, conclusions and recommendations of the study on risks and risk mitigation measures in social media use by mobile operators in Kenya. The objectives of the study were to determine the extent to which mobile telephone operators use social media, to identify the risks associated with social media use by the mobile telephone operators in Kenya and to establish the risk mitigation measures used by the mobile telephone operators to mitigate social media risks.

5.2 Summary of the findings

The study adopted a descriptive survey research design with data collected from the four mobile telephone operators in Kenya namely Safaricom Ltd, Airtel, Orange and Yumobile. From each company, the heads of marketing, human resource, customer care, information technology, operations, social media and legal departments were identified as the respondents. The study utilized primary data that was collected through a self-administered structured questionnaire. The questionnaire data was then analyzed using descriptive statistics with the help of the Statistical Package for Social Sciences (SPSS) software.

The study revealed that social media has been widely adopted by all the four mobile telephone operators in Kenya. Facebook and LinkedIn are used to a great extent while twitter, YouTube and internal enterprise solutions are moderately used by the mobile operators. These social media platforms are used to a great extent to market products and services, communicate information to customers as well as deliver customer services online. On the other hand, they are moderately used for knowledge sharing among employees, communication of information to employees and for personal use by employees.

The ability to share user generated content and the interactive nature of social media has opened up opportunities that the mobile operators in Kenya have benefited from. The study revealed that through social media, they have been able to do viral marketing, improve customer relations, develop innovative products through customer feedback, get product and service recommendations, share knowledge among employees and get referrals to potential customers.

While social media has offered opportunities and benefits to the mobile telephone operators in Kenya, it has also exposed them to certain risks. The findings indicated that that all the four mobile operators are exposed to social engineering attacks, disclosure of intellectual property and confidential information, identity theft, spreading of malware and risks of non-compliance to privacy laws. They rate social engineering attacks, disclosure of confidential information, disclosure of intellectual property and identity theft as moderate risks and consider spreading of malware and non-compliance to privacy laws as low risks. The risks identified in this study are in line with those discussed in the literature review section as risks of social media use in an organization. The study also revealed that the state of awareness of employees of the four mobile operators on social media risks is moderate.

On the risk mitigation measures, the findings indicated that the four mobile operators in Kenya have put in place risk mitigation measures against social media risks. Enforcement of the social media policy and activity monitoring are the most used social media risk mitigation measure. Training and use of symbols in risk communication to staff and customers are moderately used. In terms of effectiveness of the risk mitigation measures, activity monitoring is highly effective while enforcement of a social media policy, use of risk communication symbols to staff and customers and training are moderately effective. The social media disaster management plan as a risk mitigation measure is barely effective in the mobile industry with only half of the mobile operators indicating that they have disaster management plans in place.

With regards to training, the findings reveal that the frequency of training on social media by the mobile operators is in mostly when employees are newly employed. 21% of the respondents indicated that employees in their organizations are trained annually while 12% are trained bi-annually.

On the responsibility of development and enforcement of the social media policy in the organization, the findings indicated that it majorly lay with the marketing department.

Lastly, the study established that a majority of employees working for the mobile operators are moderately prepared in case of a social media breach or attack.

5.3 Conclusions

The study concludes that social media has largely been adopted by the mobile telephone operator firms in Kenya and is used to a great extent. Customer oriented activities such as marketing, product development and customer service use social media to a great extent while employee centric activities such as knowledge shairing, information communication among employees and personal use by employees are moderately undertaken by the mobile operators firms.

Secondly, the social media risks that mobile telephone operators are exposed to are social engineering attacks, disclosure of confidential information, disclosure intellectual property, spreading of malware and non-compliance to privacy laws. Further, the study also concludes that the level of employee awareness on social media risks is moderate.

Lastly, the social media risk mitigation measures that have been put in place by the mobile telephone operators in Kenya are enforcement of the social media policy, activity monitoring, training and risk communication using symbols. The most effective risk mitigation measures are enforcement of the social media policy and activity monitoring. These are also the most widely used social media risk mitigation measures. Other risk mitigation measures such as training and risk communication using symbols are moderately used. It is also worth noting that a number of risk mitigation measures are used by the mobile operators at the same time. As a result to effectively mitigate businesses from social media risks it is important to put in place a multidimensional approach to risk mitigation and management.

5.4 Recommendations

The first step towards mitigating social media risks is to create awareness about the risks and the potential impact of those risks to the organization and to the users. Users who are aware of the risks and the potential impact of the risks are more vigilant in identifying the risks and are more likely to use social media appropriately. They are also more likely to support the organizations efforts in mitigating social media risks. The study revealed that the employees in the mobile telephone operators firms are moderately aware of the risks in using social media. It therefore follows that there is a likelihood of inappropriate use of social media by the employees of the mobile telephone operator firms because of limited awareness of the risks involved. Their vigilance and support for risk mitigation measures is also likely to be limited because they are not fully aware of the risks and the potential impact of those risks. This study therefore recommends that mobile operator firms in Kenya should improve the level of social media risks awareness in their organizations. The state of awareness may be improved through training. However, as revealed by the study, a majority of the mobile operator firms only conduct training on social media when employees are newly employed. Because social media is dynamic and covers a wide range of topics, this study also recommends that the training models used by the mobile telephone operator firms should not only have the trainings conducted when the employees are newly employed but should also include refresher sessions annually or bi-annually. This will ensure that employees understand social media risks, the potential impact of exposure those risks and consequently use it appropriately in the organization.

The study revealed that a majority of the mobile telephone operator firms have allocated the responsibility of social media policy development and enforcement to their marketing departments. However, the social media policy cuts across all the departments in an organization including HR, legal, communications among others. Additionally, while employers may want to mitigate social media risks and protect themselves through policies and procedures, employees also have a right to personal existence and opinions which may be expressed on social media platforms outside the boundaries of official business operations. This study therefore recommends that mobile telephone operators adopt a well co-ordinated and integrated interdepartmental approach towards social media policy development and enforcement. Interdepartmental consultations creates an environment of inclusivity and the balance between the employers' needs to mitigate social media risks and the employees' rights to opinions thus making the social media policy content acceptable to all parties. Its implementation and enforcement in risk mitigation therefore becomes more effective.

Lastly, the mobile operators that do not currently have disaster management plans should put them in place. The study revealed that only half of the mobile operators in Kenya have social media disaster management plans and that in case of a security breach or attack, they are averagely prepared. In order to reduce the impact of a security breach or attack, it is important to have clear response plans and procedures to guide the managerial decisions and subsequently save the organization from potential irredeemable losses.

5.5 Limitations of the Study

During the process of data collection, there was a lot of anxiety in the mobile phone industry because of the acquisitions that were taking place during the time of the research. Airtel was in the process of acquiring the Yu mobile customers and Safaricom was in the process of acquiring the Yu mobile telecommunication infrastructure during the time of data collection. This anxiety may have been caused the respondents to withhold some information that may have been important to this study thus limiting the findings of this study.

The study relied on the respondents' perception to determine the risk levels of identified risks and not on a scientific methodology of risk assessment. These perceptions may vary depending on the understanding of the respondents' on the risks and may result into inaccurate risk ratings. It is therefore possible that a scientific risk assessment process may result into different risk ratings.

5.6 Recommendations for Further Studies

Since the study was focused on social media benefits, risks and risk mitigation measures in the mobile industry in Kenya, the study recommends that;

i. Similar studies should be done in other industries like the media industry for comparison purposes.

ii. More studies should also be done on the challenges facing social media management in organizations in Kenya.

REFERENCES

Aula, P. (2010): ‘Social media, reputation Risk and Ambient Publicity Management’, Vol 38, No 6, Strategy and Leadership, pp 43-9.

Bener, A.B. (2000): ‘Risk perception, trust and credibility: a case in internet banking’, PhD thesis, London School of Economics and Political Sciences, London.

Boyd,M. and Ellison, N.N. (2007):‘Social Network Sites: Definition, History and Scholarship’, Journal of Computer Mediated Communication, Vol 13 No.1

BITS (2011): ‘Social Media Risks and Mitigation’, A Division of the Financial Services Round Table, Pennysylvania.

Brown, J.S. and Duguid, P. (2000): ‘The Social Life of Information’, HBS Press, Boston.

Burford, S. (2012): ‘Using Social Media to Extend Information Practice in the Information Sector’, Social and Information Research, Emerald Group Publishing, *Library and Information Science,* Vol 5, pp 215-238.

Burshtein, S. and Turco, A. (2010): ‘Communication on web goes 2.0 ways’, September 8, available at:www.blakes.com/English/view_disc.asp?ID=4196 (Accessed 15 April)

Chebet, D. (2012): ‘Social Media as a Strategic Communication Tool by Safaricom Ltd’, Unpublished MBA Project, University of Nairobi

Chelia J. and Field J. (2012): ‘Social Media Misuse, A ticking Time Bomb for Employers’, Sydney, Australia.

Cisco (2012): ‘Securing Web 2.0 and Social Networking for Enterprise IT’, San Jose, America.

Clearswift (2007a): ‘15 Common Mistakes in Web Security: Enterprise Vulnerabilities that invite attack’, available at http://www.newbase.com au/15% 20 Common% 20 Mistakes% 20in % 20web%20 Security.pdf (accessed 14th April, 2013).

ClearSwift (2007b): ‘ Content Security 2.0: The Impact of Web 2.0 on Corporate Security’, available at:www.computerworlduk.com/cmsdata/whitepaers/5450/clearswift survey report_us_07.pdf (accessed 14 April, 2013).

ClearSwift (2007c): ‘Data leakage: the stealth threat to business’, available at: http://i.i.com.com/ cnwk.id/html/itp/clearswift_data_leakage.pdf (accessed 14 April 2013).

ClearSwift (2007d): ‘Demystifying Web 2.0: opportunities, threats, defenses’, available at:http://resources.clearswift.com/ExternalContent/C12CUST/Clearswift/9514/200707_DemystifyingWeb2[1].0_US_1062190.pdf (accessed 14 April 2013).

Duncan et al (1992): ‘Private Lives and Public Policies’, Washington DC, National Academic Press, pp22.

FERF and Thorton G. (2011): ‘Social Media and its Associated Risks’, Danvers, U.S.A.

Getting, B. (2007):‘Basic Definitions: Web 1.0, Web 2.0, Web 3.0’, available at http://www.practicalcommerce.com/articles/464/BasicDefinitions_web_1.0,web_2.0,web_3.0.

Gorge, M.(2007): ‘Security for third level education organizations and other educational bodies’, *Computer Fraud Security*,Vol.2007 No.7,pp.6-9

Granovetter, M. (2004): ‘The impact of social structure on economic outcomes’, *Journal of Economic Perspectives*, Vol 19 No. 1,pp 33-50

Horrigan, J. (2007): ‘A typology of Information and Communication Users,’ PWE/Internet and American life Project, research report, Princeton Survey Research Association.

Kanter, B. (2010): ‘The Networked Non-Profit: Connecting with Social Media to Drive Change’. San Francisco, Jassey-Bass.

Kaplan, A. and Haenlein M. (2010): ‘Users of the World Unite! The Challenges and Opportunities of Social Media’, Business Horizons, pp 59-68, Vol 53, Issue 1, 2010.

Kasperskylab (2008): ‘ Security Trends 2008’,available at:http ://viewer.bitpipe .com AccessId=7319425(Accessed 15 April 2013)

Laudon, K., Laudon, J. and Dass R. (2010): ‘Management Information Systems’, 11th Edition (Pearson), pp 526-533.

Leitch,S and Warren,M (2006): ‘Social engineering and its impact via the internet’, in Valli,C. and Woodward, A. (Eds), *Proceedings of the 4th Australian Information Security Management Conference, Western Australia:Edith Cowan University,Perth,pp 184-9*

Lippa, R.A. (1994): ‘ Introduction to Social Psychology’, Wadsworth, Belmont, CA.

Lock, D. (2008): ‘ Project management’, 9th Edition (Gower Publishing), pp 99-101.

Maggianni, R. (2012): ‘Social Media and its Effects on Communication: Multidimensional Interactions have altered the basic rules of communication’, accessed from http//:www.solari.net (Accessed 15 April 2013)

Matuszak, G. (2007): ‘Enterprise 2.0: The Benefits and Challenges of Adoption’, whitepaper, KPMG LLP International, May, available at http:// us.kpmg.com/microsite/attachments/2008/Enterprise2.0_Adaptation.pdf (Accessed 15th April, 2013).

McAffee, A. (2009): ‘Enterprise 2.0 New Collaborative Tools for Your Organization’s Toughest Challenges’. Boston, America.

Message Labs (2007a): ‘Online Social Networking; The employer’s dilemma’, available at http://www.downloadsmessagelabs.com/silokoruik/wss_whitepaper_socialnetworking_legal_a4_final.pdf (Accessed 26th March, 2013).

Mugenda, O. and Mugenda, A. (2003): ‘Research Methods; Quantitative and Qualitative Approaches’, Africa Centre for Technology Studies, Nairobi, Kenya, pp 117, 173-198.

Mwangi, T. (2012):‘Influence of Social Media on Customer Service at Safaricom Ltd’, Unpublished MBA Project, University of Nairobi.

Onn et al (2005): ‘Privacy in the Digital Environment’, *Haifa Centre of Law and Technology,* pp 1-12.

O’Reilly,T.(2005): ‘What is Web 2.0? Design patterns and business models for the next generation of software’,available at www.oreillynet.com/lpt/a/6228 (accessed 15 April,2013).

Orlikowski,W.J. (2002): ‘Knowing in Practice: enacting a collective capability in distributed organizing’, Organizational Science,Vol.13 No.3,pp.249-73.

Pattinson, M. and Anderson, G. (2007): ‘How well are information risks being communicated to your computer end-users?’, available at www.emeraldinsight.com/0968-5227.htm (accessed 15 April, 2013).

Parise, S., Guinan, P.J. and Weinberg, B.D. (2008): ‘The secrets of marketing in a web 2.0 world’, *The Wall Street Journal*, Vol 1 R4, December 15.

Petty, R. (2012): ‘Using the Law to protect the Brand on Social Media Sites, A Three “M” Framework for Marketing Managers’, Massachusetts, USA.

Ponemon Institute (2011): ‘Global Survey on Social Media Risks: Survey of IT and IT Practitioners’, Ponemon Institute Research Report, Canada.

Radcliff, D. (2007): ‘Are you Watching ?’ SC Magazine, September , pp 40-3.

Rein, W. (2011): ‘Facebook, YouTube and whateverisnext.com: Are Social Media Sites really the internet’s wild west (again)?’, Mass Media Headlines, January, pp 6-8 available at www.wileyrein.com/publications.cfm?sp=articles 8 newsletter=5 & id=6724 (Accessed March 26th).

Rudman, J. (2009): ‘Incremental Risks in Web 2.0 Applications,’ Stellenbosch, South Africa.

Smith, D. (2008): ‘Web 2.0 and Beyond: Evolving the Discussion, research report, Gartner 24th January, available at http://www.gartner.com/Display/Document? (accessed 15th April, 2013).

Shirky, C. (2008): ‘Here Comes Everybody’,The Power of Organising without Organisations, Penguin Books, New York, NY.

Symantec (2011): ‘Social networking, security and your business: a guide for IT managers’, Lansdowne Court, United Kingdom.

Tapscott, D. and Williams, A.D. (2006): ‘Wikinomics: How Mass Collaboration Changes Everything’, Portfolio, New York, NY.

Vander Veer, E.A. (2008): ‘Facebook: The missing manual’, Sebastopol, Pogue Press.

Wasike, J. (2012): ‘Social Media Ethical Issues: Role of a Librarian’, Catholic University of Eastern Africa, Nairobi, Kenya.

Wellman, B. (2001): ‘Computer Networks as Social Networks, Science 293, (September 14, 2001):2031-34.

Zyl, A. (2008): ‘The Impact of Social Networking 2.0 on Organizations’, Stellenbosch, South Africa.

http://*businessdailyafrica.com/opinion*. Accessed 2nd April, 2013.

http://*socialbakers.com/facebook-statistics/kenya*. Accessed 2nd April, 2013.

http:*socialbakers.com/twitter-country/Kenya*. Accessed 2nd April, 2013.

http://*gartner.com/DisplayDocument?ref_gsearch*.Accessed 15th April, 2013.

APPENDICES

Appendix 1: Questionnaire Guide

Section A: Background information

1. Name of Respondent……………………………………………………………………

2. Name of organization……………………………………………………………………

3. Position of Respondent in the organization………………………………………………

4. Number of Years Worked in the organization……………………………………………

Section B: Social Media use and its benefits to the Organization

1.) On a scale of 1 to 5 to what extent are the following social media platforms used in your organization?

1=No Extent at All 2=Low Extent 3=Average Extent 4=Great Extent

5= Very Great Extent

Social Media Platform Use	**Extent of Use**				
	1	**2**	**3**	**4**	**5**
Facebook					
LinkedIn					
Twitter					
YouTube					
Internal Enterprise 2.0 Solution					
Other (Please Specify)					

2.) On a scale of 1 to 5 to what extent is social media used in the following ways in your organization?

1=No Extent at All 2=Low Extent 3=Average Extent 4=Great Extent

5= Very Great Extent

Social Media Use	**Extent of Use**				
	1	**2**	**3**	**4**	**5**
Customer service platform					
Communication of information to customers					
Communication of information to employees					
Marketing of products and Services					
Knowledge sharing among employees					
Personal use by employees					
Other(Please Specify)					

3.) On a scale of 1 to 5 to what extent does your organization benefit from the following uses of social media?

1=No Extent at All 2=Low Extent 3=Average Extent 4=Great Extent

5= Very Great Extent

Benefits of Social Media	**Extent of Benefit**				
	1	**2**	**3**	**4**	**5**
Referrals and Introductions to Potential Customers					
Recommendations of Products and Services to Potential Customers					
Recommendations of Potential Employees					
Knowledge Shairing within the Organization					
Maintaining Staff Morale and Job Satisfaction					
Improvement of Customer Relations through Customer Feedback					
Viral Marketing					
Development of Innovative Products through Customer Feedback					

Section C: Social Media Risks

4.) On a scale of 1 to 5 how would you rate the following risks of social media use in your organization?

1=No Risk at All 2=Low Risk 3=Average Risk 4=High Risk

5= Very High Risk

Risks of Social Media	**Extent of Risk**				
	1	**2**	**3**	**4**	**5**
Risks of Non-Compliance to Privacy Laws in Kenya					
Identity Theft					
Social Engineering Attacks					
Spreading of Malware					
Disclosure of Intellectual Property					
Disclosure of Confidential Information					
Reduced Productivity					
Misinformation to Customers and Other Stakeholders					
Other (Please Specify)					

5.) On a scale of 1 to 5 how would you describe the state of awareness of employees of these risks in your organization? Please choose one.

- □ **1=Not Aware at All**
- □ **2=Low State of Awareness**
- □ **3=Average State of Awareness**
- □ **4= High State of Awareness**
- □ **5= Very High State of Awareness**

Section D: Social Media Risk Mitigation Measures

6.) On a scale of 1 to 5 to what extent do you use the following risk mitigation measures to mitigate the risks in social media use in your organization?

1=No Extent at All 2=Low Extent 3=Average Extent 4=Great Extent

5= Very Great Extent

Risk Mitigation Measures	**Extent of Use**				
	1	**2**	**3**	**4**	**5**
Training					
Activity Monitoring on Social Media Sites					
Use of Symbols in Risk Communication to Staff and Customers					
Enforcement of Social Media Policy					
Development of a Social Media Disaster Management Plan					
Other (Please Specify)					

7.) How frequently do you conduct training on social media use in your organization?

- ❑ When Newly Employed
- ❑ Annually
- ❑ Bi-Annually
- ❑ Other (Please Specify)

8.) In what ways do you monitor activity on social media sites in the organization?

- ❑ Content monitoring on social media sites by Employees
- ❑ Through software tools
- ❑ Outsourced monitoring experts
- ❑ All the Above
- ❑ Other (Please Specify)

9.) Who is responsible for developing the social media policy in the organization?

- ❑ HR
- ❑ Marketing
- ❑ Social Media Department
- ❑ Legal Department
- ❑ Other please specify
- ❑ All the Above through a Co-ordinated approach

10.) Who is responsible for enforcing the social media policy in the organization?

- ❑ HR

□ Legal

□ Social Media Department

□ Marketing

□ Other (Please Specify)

11.) Do you have a social media disaster management plan.

□ Yes

□ No

12.) How would you consider your state of preparedness incase of breach, attack or fraud?

□ **1=Not Prepared**

□ **2=Ill Prepared**

□ **3=Averagely Prepared**

□ **4= Highly Prepared**

□ **5= Very Highly Prepared**