EFFECTS OF CYBERCRIME MANAGEMENT ON INFORMATION SECURITY OF SELECTED HOTELS IN NAIROBI KENYA

MOSES MURAYA

SBE/PGH/009/11

A THESIS SUBMITTED TO THE SCHOOL OF TOURISM, HOSPITALITY AND EVENT MANAGEMENT, DEPARTMENT OF HOTEL AND HOSPITALITY MANAGEMENT IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF A DEGREE OF MASTER OF PHILOSOPHY IN HOSPITALITY MANAGEMENT, MOI UNIVERSITY

NOVEMBER, 2014

Quote

"Mind is the Master power that molds' and makes,

And Man is Mind, and evermore he takes

The tool of thought, and, shaping what he wills,

Brings forth a thousand joys, a thousand ills:

He thinks in secret, and it comes to pass:

The environment is but his looking-glass."

As A Man Thinketh By James Allen

DECLARATION

This thesis is my original work and has not been presented for a degree in any other university. No part of this thesis may be reproduced without the prior written permission of the author and/or Moi University.

Moses Muraya Date: ……..

Signature: …….

Declaration by Supervisors

This thesis has been submitted with our approval as University Supervisors.

Dr. Zakayo Mapelu Date: …….

Signature: ……

University Of Eldoret, Kenya

Dr. Tirong arap Tanui Date:…….

Signature: ……

Moi University, Eldoret, Kenya

DEDICATION

I dedicate this work to Muraya‘s family, my fiancé and all my friends because you made me who I am and for your love and support you have given and continue giving me.

ABSTRACT

Information assets are critical to any business and paramount to the survival of any organization in today's globalized digital economy. Unauthorized information leak, which is intolerable, often indicates poor or inadequate information security measures. Internationally, hotels have in recent years become targets for cybercrimes as they form rich grounds of information and data needed to commit cyber-crimes. Cybercrime management can be divided into aspects such as cyber-threats, security frameworks policies, and management appreciation of the business value of IT investments. These factors have a significant influence on an organization's information security. The purpose of this study was to investigate the effects of cybercrimes on information security of selected hotels in Nairobi Kenya. The objectives of the study were: To investigate the existing security framework policies adopted by selected hotels in Kenya to ensure information security; To establish the common types of cyber-threats and their effect on information security; and To determine management appreciation of the business value of IT investments in ensuring information security. Descriptive and explanatory research design was adopted for the study. The target population was 935 and a sample size 280 from four selected hotels was used. Purposive sampling was used to select hotels for the study, stratified sampling to stratify respondents into departments and simple random sampling was used to select individual respondents. Semi-structured questionnaires were used to collect data from the management and the IT department personnel while structured questionnaires were used for the employees. Secondary sources of data were used to supplement data collected from the field. The data collection instruments were tested using Cronbach’s alpha for reliability and a pilot study was used to test for validity of the instruments. The data were analyzed using descriptive statistics, factor analysis and multiple regression. From data analysis the regression model indicated that three aspects of cybercrimes explained to a large extent the variance of information security. Further analysis of the data revealed that both cyber-threats and management appreciation affected information security with cyber threat having the highest influence. The study concluded that cyber-threats such as malware strongly influenced information security, followed by a management appreciation of the business value of IT investments in terms of budget allocation as the strongest influences of information security. These are consistent with and supports prior research that these aspects of cybercrime affected information security of organizations in other countries. The study recommends a regular (monthly) and complete review and full implementation of information security structures, regular and collective collaboration of hotels and cybercrime police on cybercrime incidences and also additional funding and support of the IT investments to ensure information security.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENT

I am grateful to God Almighty for keeping and guiding me through the obstacles that came my way. I am also grateful to my supervisors Dr. Zakayo Mapelu and Dr. Tirong arap Tanui who encouraged me when I faced challenges in my research, and also for the whole department of hotels and hospitality management for nurturing me till where I am today.

LIST OF ABBREVIATIONS

CAK – Communication Authority of Kenya

CBD - Central Business District

DCSM - Data Centric Security Model

DDoS - Distributed Denial of Service

ICT - Information Communication Technology

IGF – Internet Governance Forum

IS – Information Security

IT -Information Technology

KRA – Kenya Revenue Authority

NDA – Non-Disclosure Agreement

PC – Personal Computer

SPSS - Statistical Program for Social Scientists

U.S. A – United States of America

OPERATIONAL DEFINITATION OF TERMS

Cybercrime - offenses that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using computers and telecommunication networks such as the Internet.

Cyber threat -any identified effort directed toward access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or a federal system without lawful authority.

Information - Information takes many forms. For the purposes of this document, it includes data stored on computers, transmitted across computer networks, printed, written, sent by post or fax, or stored on removable devices.

Information security - is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction

CHAPTER ONE

INTRODUCTION

1.0 Overview

The chapter will discuss the background of the study, the problem statement, the purpose of the study, research objectives, the rationale of the study, the importance of the study, assumptions of the study, and the limitations of the study.

1.1 Background of the Study

Information technology offers businesses and countries avenues for growth economically and progress socially. Business's ability to remain competitive is now largely determined by the ability to develop, commercialize and capture economic benefits through technology adoption and innovations (Ekaterina, 2010). This has led to the reshaping of the business environment as technology; economic pressures and competition have resulted in quicker and more efficient ways of conducting business. The information age has therefore been born, with global competition, sharing of sensitive information between the business to businesses and business to customers becoming the norm (Ajibuwa, n.d.).

The computer has become etched in our day to day lives, affecting every aspect of our lives from communications sector, the education sector, the medical sector and even items as automatic machines such as Automatic Teller Machines, automatic cooking machines, such as microwaves (Philip, 2008). Kenya recognized the role of ICT to attain its vision 2030 and has indeed placed ICT as one of the main pillars of development (GOK, 2008). Also, the country has seen major investments in ICT infrastructure through the development of the fiber optic cables together with the

terrestrial cables that have resulted in increased speeds of connectivity for internet users.

However, despite the enormous benefits that have come to businesses due to Internet connections, an avenue has been opened that give malicious internet users increased opportunities for targeting their victims more easily, undetected and in large numbers (Abagnale & Mitnick, 2005). According to Semaj (2012), Kenya's former Information Principal Secretary, Dr. Bitange Ndemo, said that high internet speeds to bring with them an increase in security risks and policies need to be developed to ensure not only wider access, but also the safety of the Kenyan internet users. As the internet connectivity in Kenya continues to blossom, the cyber security threats continue being more sophisticated and dynamic in their nature.

Cybercrime involves all crimes that are perpetrated through the use of the computer and computer systems or even through the Internet. These crimes are aimed at compromising the confidentiality, the availability and the integrity of computer data and systems. In addition cybercrimes includes also the crimes that infringe on the copyright and trademark related offences and also the crimes that are classified under content related offences. Cybercrimes can be classified as crime against individuals which are targeted at persons and include email spoofing, spamming, cyber stalking and harassment; cybercrime against property and this involves all crimes such as credit card frauds, intellectual property crimes, and internet time theft; cybercrime against organizations which includes unauthorized computer access, virus attacks, email bombing, salami attacks, Trojan horse, data diddling among others; cybercrimes against society which includes forgery using computers, cyber terrorism which is aimed at government institutions and services provided through the internet, cyber laundering, and web jacking which is gaining of access over another website.

According to Symantec Corporation (2011) study on global cybercrime, they estimated the global cost of cybercrime amounted to approximately $388 billion in terms of financial losses and time lost. This figure is higher than the total global black market of marijuana, heroin and cocaine combined which is an estimated $288 billion. The report also continues to say that over 69 percent of online adults during their lifetime have been a victim of cybercrime. Also there are over one million cybercrime victims every day and the increase in attacks is now targeted to the mobile device users, social network users because of their lack of protection (Symantec Corporation, 2011).

In Kenya, the Price Waterhouse Coopers report (Muema, 2012) indicated that cybercrime ranked among the top four of the economic crimes committed in Kenya. They equated the cost of cybercrime to be about Ksh 3 billion every year. This statistics reflects an increase in cybercrime cases happening in Kenya where several attacks have been experienced such as the hacking of Deputy Presidents twitter account and The Kenya Defense Force website by a group called anonymous among other hackings of key government websites such as central banks website. This could be attributed to the increase in connectivity speeds and the adoption of technology by businesses in Kenya. However this change has not seen an equivalent increase in protection from cybercrime threats by businesses and individuals (Muema, 2012).

Among the businesses that have seen increased target by cybercrime fraudsters are hospitality businesses, according to Trustwave 2012 Global Security report, and retail businesses which accounted for 85 percent of data breach. In Kenya the hospitality industry is a key contributor to the country's Gross Domestic Product (GDP). According Kenya National Bureau of Statistics (2012), the tourism industry earned Kenyan economy around 97.9 billion in 2011 with hotels and restaurants earning the

country 50.557 billion. In 2011 the hotels and restaurant grew by 5.0 percent by GDP by industry and a total of 1.7 percent contribution to GDP by activity. The above statistics indicate the importance of the hospitality sector to the Kenyan economy. Also the recent political instability like the post-election violence and the increase in travel advisory against the country due to terrorism threats has seen the tourism industry and the hotel sector suffer as visitor numbers dwindle with some hotels even forced to close down. This indicates how fragile the Kenyan tourism industry is to external forces and cybercrime could be an emerging threat that could contribute to imbalance to the industry. The global hospitality industry experienced majority of the cybercrime incidences accounting to 52 percent (Barnett et al, 2012). White Lodging Services Corp data breach that exposed about 14 United States hotels to credit card hacking scheme is an example of hotels falling victim to cybercrimes (Wiener-Bronner, 2014). The increased attacks on the hospitality industry could be attributed to the lax security measures hospitality businesses place on data security as this does not fall among the core services offered by hotels (Greenberg, 2010).

According to Greenberg (2010), he argues that in recent years there has been a spike in hacking incidents targeting hotels and resorts because they have relatively unprotected sources of up to millions of credit account details. Therefore hotels are targets for cybercrimes as they form rich grounds of information and data needed to commit cybercrimes. This is because hotels handle a variety of information concerning the client from personal information, credit card details, purchase behavior of the client, their medical conditions from allergies to lifestyle diseases, clients address and contacts among others (The Hospitality Sector, 2012). In addition, the hotel houses data concerning its employees, hotels business partners from goods and service suppliers to business that provide the hotel with business. For a cybercriminal

who knows which information to look for, a hotel provides an easy and a rich goldmine of data for them to conduct any fraud they wish from impersonation, cyber stalking, financial crimes and many more (Goudie, 2011). A scenario to depict the ease of information breach can be explained in the following scenario. When identity thieves walk into a hotel lobby they see opportunity: distracted business travelers and relaxed vacationers who are paying little attention to their wallets, private documents or their personal security; a workforce with high turnover and minimal background checks if any; and easy access to hotel guest areas, guest rooms, and hotel computers (Levin & Hudak, 2009). With the hotels systems being vulnerable and relatively unprotected, hackers specifically target hospitality sector for they are easily available and lucrative, leading to Nicholas Percoco to say in the Black Hat Security Conference In Arlington, VA "the hospitality industry was the flavor of the year for cybercrime" (Greenberg, 2010).

Businesses sometimes consider spending on security to be a pure cost that does not bring tangible returns and those that invest in it will usually choose the cheapest option (Needleman, 2012). Therefore it's of paramount importance for businesses to protect themselves from cybercrime as the consequences of an information breach can be dire to the company (Burgess, & Power, 2008). This can be in terms of direct loss of hotel's finances, to a tarnished brand image, loss of company secrets, litigations against the hotel by customers and even loss of business that may lead to closure of the business (Kitten, 2012; Tia, 2011; Petrocelli, 2005).

Even though hotels do not consider data protection as core service they provide, the nature of the information hotels handle requires high levels of protection as this information is an invaluable asset of the company which can turn to a costly liability if not well handled. Customers also will not feel secure about their information they

are required to divulge to hotels and also the information they carry with them in their computer devices. Customers will fear for their computers to be infected with malware or even being hacked when accessing unsecured hotel internet network (Ekaterina, 2010; Philip, 2008).

Other impacts of cybercrimes include the erosion of trust between consumers and businesses operating in the web environment due to the increase in internet crime as Grabner-Kraeuter (2002) observed that "In essence, consumers simply do not trust most Web providers enough to engage in relationship exchanges with them." The fragile trust in using e-commerce has been put in balance by the increasing cybercrime and many organizations and governmental agencies are now taking steps to combat cybercrimes to restore customer confidence.

In addition, cybercrime has been considered as a hindrance to the growth of e-commerce due to the increased presence of cybercrimes and will impact negatively the confidence of consumers in the search of information and purchase of products and services online. This is because customers will be reluctant to provide sensitive information and credit card numbers online unless retailers and service providers put in place measures to protect this information.

The cyber criminals constitute of various groups or categories. This division may be justified on the basis of the objective that they have in their mind for committing the crime. The first category is a classification of children and adolescent hackers aged between the ages of 6-18 years. This category is characterised by inquisitiveness to know and explore things and thus the need to prove themselves as outstanding to their peers. The second category includes the organised hackers whose aim is to fulfil a certain objective for example WikiLeaks is as a result of the hackers objective of free

information for everyone. Professional hackers or crackers form another category that is motivated by the benefits of money and the last category is the discontented employees whose directive is an act of revenge against their employer (Pati, n.d).

Furnell 2001 also classified hackers and their motivations for committing cybercrimes. He classified hackers into three categories of "black hats", "white hats" and "grey hats". Black hats include whose intrusion into the system is malicious and clearly unauthorized and sometimes they are referred to as the "dark side" hackers. The white hats otherwise known as "ethical hackers" work for the good of system security while the "grey hats" fall between the previous two categories and their intentions for engaging in cybercrimes are unclear and could change. The motivations of these hackers range from the need for a challenge, ego, espionage, ideology, mischief, money and revenge (Ngafeeson**,** n.d).

Conferences and workshops have been held in the Kenya such as the ICT Security Africa summit 2010 that was held at Sarova Whitesands Beach Resort in Mombasa and whose aim and theme was "Global Best Practices to Enhance Cyber Security and Protect Critical Information Infrastructures and Assets across Africa". Communication Authority of Kenya (CAK) also organized a presentation at 2010 Kenya Internet Governance Forum (IGF) to address cybercrime, cyber security and privacy.

Criminal law in recent years has struggled to be at par with the ever expanding technologies of cyberspace. The ambiguity of defining cybercrime in relation to computers and the internet has caused problems to law-makers in many countries throughout the world. According to Sterling (1992), he wrote in his book the Hacker Crackdown, which was chronicled in "Operation Sun-Devil" in U.S., that the

inadequate and antiquated laws severely hampered law enforcement activities and ultimately embarrassed the U.S government. Most of the arrested hackers received little if any punishment from the courts because the alleged stolen information was actually non-confidential public material (Rogers, 2001). In addition, most of the legislators do not understand the technology or the ramifications of security breaches and some of the legislators have reacted conservatively and resisted changes in the criminal code with a good example being the Canadian legislators (Davis & Hutchison, 1999). The law must therefore keep pace with technology and clearly define what constitutes a criminal act and prove beyond reasonable doubt that the crime has taken place.

In the year 2010 the Kenyan government, CAK and the cybercrime unit of Criminal Investigation Department (CID) have put in place measures to address cybercrime menace and threats in the country. CAK formerly Communication Commission of Kenya (CCK) announced that it would start monitoring online activity for cybercrimes and prosecute those committing crimes using digital technology be it computers, mobile phones or the internet service providers (Magutu, Ondimu, & Ipu, 2011).

1.3 Problem Statement

The hospitality industry shares many of the same data security vulnerabilities as the retail industry — accepting and storing cardholder information and personal information collected through participation in loyalty and rewards programs — yet lags in the adoption of data security practices, which makes it an attractive target for cybercriminals (JJ, 2010). The most common problem in hotels is that data is not secure; rather, it generally resides in applications and databases as unsecured, clear-

text data in most case, whether it's payment card information or other sensitive consumer or employee information.

Hospitality managers and employees in Kenya generally lack adequate and real-time information on cyber threats. This is formed by the manager's limited knowledge on the range of cyber threats that are faced by organizations. This could be caused by the lack of regular and current industry by industry statistics on cybercrimes in the country and the severity of cyber breaches for organizations. In addition to that most of the employees and managers lack knowledge of cybercrime laws affecting their businesses.

This has resulted in managers in hospitality businesses lacking the appreciation of the seriousness of cyber threats which is evidenced by the lack of adequate funding and staffing of the IT department with some of the establishments running without IT department. The implementation of information security policies also faces the challenge of lack of support from the establishment's management in terms of infrastructure development and budgeting.

This has caused inadequate or non-existent security systems and frameworks by hospitality business which has resulted in the danger of data breaches and the consequences that later arise. This is because hospitality businesses sometimes consider spending on security to be a cost that does not bring tangible returns and those that invest in information security will usually choose the cheapest option available. Therefore the lack of adequate knowledge of cyber threats, the low appreciation and support by executive managers for the IT department, and the inadequate security systems and frameworks has collectively contributed to the increased information insecurity in the Kenyan hotels as presented in figure 1.1

below. Therefore this study aims to find out how Kenyan hotels are managing cybercrimes and information security in their businesses.

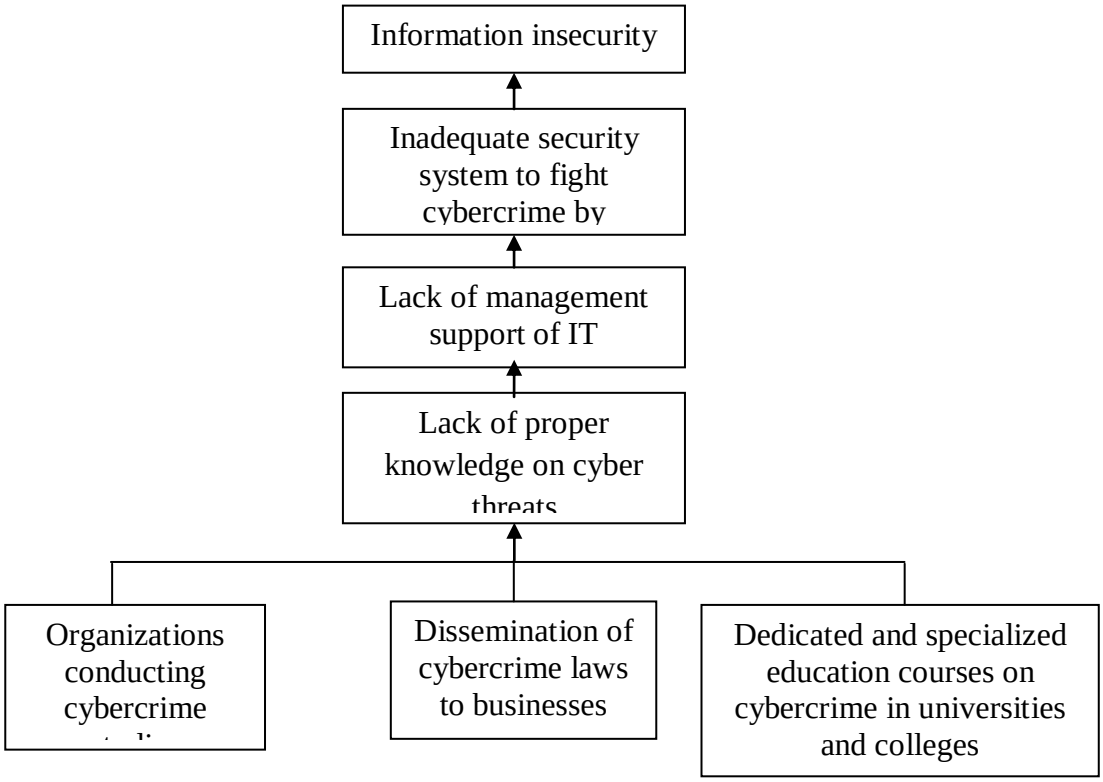

Figure 1. 1: Information Insecurity Problem Tree

Source: *Author, 2013*

1.4 Purpose of the Study

The purpose of the study was to find out extent of the effects of cybercrime management on information security of selected hotels in Kenya.

1.5 Main Research Objectives

To investigate the effects of cybercrime management on information security of selected hotels in Kenya.

1.5.1 Specific objectives of the study

i. To investigate the nature of security framework policies that ensure information security of selected hotels in Kenya
ii. To establish the relationship between cyber threats and their effect on information security of the selected hotels in Kenya.
iii. To determine the executive management's appreciation of IT investments to ensure information security in selected hotels in Kenya.

1.5.2 Research hypothesis

Ho_1. The nature of security framework policies does not ensure information security of selected hotels in Kenya.

Ho_2. Cyber threats do not affect information security of selected hotels in Kenya

Ho_3. Executive management appreciation of IT investments do not affect information security of selected hotels in Kenya.

1.6 Justification of the Study

Information insecurity continues to pose a significant threat to the hospitality industry in Kenya. Therefore the findings of this study are helpful for the Kenyan hospitality sector as it gives insight to information insecurity that results from cybercrime in the hotel sector. This will help manager's better plan on information security policies and provide more effective avenues of detection and prevention of crimes such as cybercrime.

Also the findings will enable the Kenyan government and the cybercrime unit of Kenya police to focus their energy on the most common forms of cybercrimes that

affect Kenyan businesses. This will enable them to develop a framework for investigation and prevention of such crimes.

The study will be of benefit to the Kenyan education sector as it will provide real and current cybercrimes and risks that are occurring in Kenya and therefore enabling them to develop researchers on how to fight such crimes. Also it will provide some case scenarios to be used by the students for practice and learning. The study will also be of benefit to the Kenya Revenue Authority (KRA) as they will be able to formulate basic information security requirements that businesses should conform to reduce the loss of revenue due to cybercrime incidences.

The legal fraternity of Kenya will benefit from the study by showing how much cybercrime can be damaging to businesses and individuals in Kenya thus help in formulating laws and policies to protect the rights of information and privacy of individuals as stipulated in the new Kenyan Constitution 2010 chapter four that outlines the bill of rights (Kenya Law Reports, 2010).

1.7 Scope of the Study

This study looked only at the effects of cybercrime on information security and was limited to computers operating on a windows operating system platform as it is the most widely adopted operating system by businesses in Kenya. It did not look at other platforms like Linux, UNIX, Macintosh Operating system or any other. Also the study's scope was limited by geographical coverage as it considered hotels in Nairobi Kenya. This was because Nairobi was among the first cities to adopt Internet use in businesses and most of the city hotels were among the first adopters of technology use in hotels. This made Nairobi to be the ideal place to conduct the study.

1.8 Assumptions of the Study

This study was carried out with the assumptions that the organizations have experienced some form of cybercrime incidence and that the cases were known by the employees. Also the respondents would cooperate in filling the questionnaires and that they would not take a very long time (over six months since when they received the questionnaire) to fill in the questionnaires given.

1.9 Limitations of the Study

The limitations that were encountered in the process of data collection included:

1. Time: The time allocated for the study to be undertaken was not sufficient to cover exhaustively all aspects related to the study. Time also limits the scope of the study in terms of geographical coverage. However the researcher overcome this by involving multiple samples and using the help of research assistants to quicken data collection.

2. Funds: The research was basically financed through personal resources which were scarce. This posed a limitation on the scope of coverage as it was confined to one region of the country. This was overcome by selecting hotels within easily accessible places and not those in parks or secluded places.

3. Past research materials: Past research on cybercrime especially in the hospitality industry especially in Africa and Kenya were not easily available and accessible both in the library and on the internet. This was overcome by utilizing the university library to access some of the materials that required subscription.

CHAPTER TWO

LITERATURE REVIEW

2.0 Overview

This chapter gives an in depth review of literature that other authors have written concerning information security, the types of cybercrimes, their mode of perpetration, and some measures businesses can take to reduce the risk of being victims of cybercrimes. This chapter reviews literature about what is being done by other countries and the Kenyan government in combating cybercrime.

2.1 Information Security

Since the early days of writing, the heads of states and military commanders understood the importance of protecting confidentiality of written correspondence, preventing tampering and ensuring authenticity of information. They used wax seals and other sealing devices to prevent tampering of information being passed on. However the late 20th and early 21st century saw the rapid advancement of ICT and e-commerce adoption by governments, businesses, and individuals and this fueled the need for better methods to protect computers and information storage, processing and transmission. This led to the emergence of academic disciplines on computer security, informational security and information assurance all with the main goal of ensuring security and reliability of information systems (Ajibuwa n.d.).

2.1.1 Basic Principles of Information Security

Information security has held three key concepts which form the core principles of information's security: confidentiality, integrity and availability. These are known as the CIA triad (Tittel, Chapple, & Stewart, 2003).

2.1.1.1 Confidentiality

In modern world, it is virtually impossible to get a driver's license, take a loan or even book hotel accommodation without disclosing a great deal of personal information such as name, address, telephone number, date of birth/age, marital status, number of children, next of kin, place of employment, medical history/special ailments among many others (Peltier, 2001). This personal information is needed to be divulged in order to transact business. Yet people place their faith that the people, businesses, or institutions they are giving these details have taken the adequate measures to protect that information from unauthorized disclosure whether accidental or intentional (Ajibuwa n.d.).

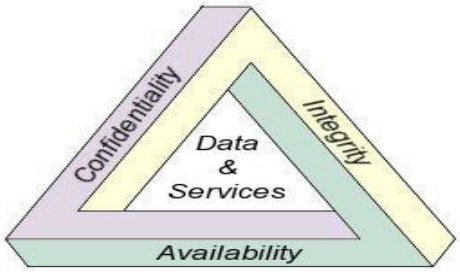

Figure 2. 1: The CIA Triad

Source (Ajibuwa n.d.)

Confidential information must only be accessed, used, copied or disclosed by persons who have been authorized to access, use and copy or disclose the information only when there is genuine need to access, manipulate or disclose that information (Cartwright et al, 2012). Anything contrary to the above circumstances leads to a confidentiality breach.

A confidentiality breach can occur due to aspects such as someone looking over another's shoulder, to a computer screen that is displaying confidential data, to a

stolen computer of an employee or storage device that contains confidential information of the company. Therefore, confidentiality is a requisite for maintaining privacy of the people whose personal information is held by the organization and organizations must use all means to ensure information protection (Ajibuwa n.d.).

Confidentiality may also be categorized to discretion of the source or sources of information. People supplying information should also ensure privacy of the information being supplied is upheld. This is because someone can intercept sensitive information from personnel that are careless in handling the information. As such proper care and precautions must be taken to ensure confidentiality (Krutz & Russell, 2003). Hotel guest also contribute to information confidentiality as most of them tend to leave their laptops and mobile phones, documents such as passports among others unattended on the reading table or bed in their rooms and sometimes in public areas. This exposes them to physical intrusion to their information like either theft or copying of data. Hotels should therefore advice their guests during checking in to keep their valuables safe and for mobile phones and laptops logged off or out of sight.

2.1.1.2 Integrity

In information security, integrity means that data should not be created, changed, or deleted without authorization. Integrity also means that data stored in one part of a database system is in agreement with other related data stored in another part of the database system (or another system). For example: a loss of integrity can occur when a database system is not properly shut down before maintenance is performed or the database server suddenly loses electrical power (Ajibuwa n.d.). Also a loss of integrity can occur when an employee accidentally, or with malicious intent, deletes important data files and also if a malicious logic software is released onto the

computer (Warren, Jennifer, & Daniel 2009). Therefore safe guards should be put in place to deter any violation of integrity by following laid down procedures when handling information. These could be access controls, secondary backing up of databases and doing regular audits to check how safe the company's most important asset is.

2.1.1.3 Availability

The concept of availability means that the information, the computing systems used to process the information, and the security controls used to protect the information are all available and functioning correctly when the information is needed. The opposite of availability is Distributed Denial of Service (DDoS) (Tittel, Chapple & Stewart 2003). There is a clear expectation by organisations that important data be available 24 hours a day, 7 days a week, 365 days a year as information is the lifeline of an organization. Without a working data protection strategy, that isn't possible (Petrocelli, 2005).

However in 2002, Donn Parker (Peltier, 2002), proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. His alternative model included confidentiality, possession or control, integrity, authenticity, availability, and utility (Cartwright et al., 2012).

2.1.2 Breaching Organizational Security

A number of organizational security breaches can occur; some of these are amplified by the use of a database because of the integrated approach to data storage and retrieval. Some of these breaches and security issues include computer viruses, unauthorized access (hacking), industrial and/or individual sabotage, accidents by

users (incompetence) which can lead to loss of access to the company's data, unproductive workforce, viral infection, theft of company secrets and inadvertent law breaking. It is therefore important for any organization to classify their information and therefore instill the right procedures to protect that information (Ajibuwa, n.d; Kerschberg, 2011).

The single most important reason to implement data protection strategies is fear of financial loss. Data is recognized as an important corporate asset that needs to be safeguarded. For example in hotels the customer details are needed for almost all transitions. Loss of information can lead to direct financial losses, such as lost sales, fines, or monetary judgments. It can also cause indirect losses from the effects of a drop in investor confidence or customers fleeing to competitors. Worse yet, stolen or altered data can result in financial effects that are not known to the company until much later. At that point, less can be done about it, magnifying the negative results (Petrocelli, 2005).

2.1.3 Classifying Information Security

It is important to note that not all information is equal and therefore not all information requires the same degree of protection. Information needs to be classified on the basis of the owner of the particular information to be classified. Next a classification policy should be developed that describes the different classification labels, criteria for the information to be assigned a particular label and should list the required security controls for each classification (Layton, 2007).

Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and

other regulatory requirements are also important considerations when classifying information (Tittel, Chapple, & Stewart, 2003). Common information security classification labels used by the business sector are: public, sensitive, private, confidential. Common information security classification labels used are: top secret, highly confidential, proprietary, internal use only and public documents (Krutz, & Russell 2003).

All employees in the organization, as well as business partners, must be trained on the classification scheme and understand the required security controls and handling procedures for each classification. The classification which a particular information asset has been assigned should be reviewed periodically to ensure the classification is still appropriate for the information and to ensure the security controls required by the classification are in place (Ajibuwa n.d.).

Table 2. 1: Data Classification Table

Document / Data Classification	Description
Top Secret	Highly sensitive internal documents e.g. pending mergers or acquisitions; investment strategies; plans or designs; that could seriously damage the organization if such information were lost or made public. Information classified as Top Secret has very restricted distribution and must be protected at all times. Security at this level is the highest possible.
Highly Confidential	Information that, if made public or even shared around the organization, could seriously impede the organization‘s operations and is considered critical to its ongoing operations. Information would include accounting information, business plans, sensitive customer information of banks, solicitors and accountants etc., patient's medical records and similar highly sensitive data. Such information should not be copied or removed from the organization‘s operational control without specific authority. Security at this level should be very high.

Proprietary	Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organization operates. Such information is normally for proprietary use to authorized personnel only. Security at this level is high.
Internal Use only	Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level is controlled but normal.
Public Documents	Information in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level is minimal.

Source: Ajibuwa n.d.

2.1.4 Types of Data That Needs To Be Secure

Securing data means understand which pieces of information need to be protected and enacting proper procedures and safeguards to keep this information safe. Managers should ask themselves what type of information is of high priority when it comes to data security (Nutt, 2007). The most common problem for hotels is that data is not secure and it generally resides in applications and databases as unsecured, clear-text data in most cases, whether it's payment card information or other sensitive consumer or employee information. The sections below discuss some of data security considerations.

2.1.4.1. Customer Information

The demands of a 21st-century business are such that customers expect the business to operate at all times. In an increasingly global economy, downtime is not tolerated by customers, who can readily take their business elsewhere. The inability of a business to operate because of a data loss, even a temporary one, is driving many

businesses to deploy extensive data protection schemes (Mayock, 2010). An example of data breach is a credit card breach of hotel chain Wyndham worldwide Corp where hackers infiltrated the chains network and systems. This led to the chain being sued by Federal Trade Commission for their lax security that exposed stored details of nearly 670,000 accounts (Kitten, 2012).

Securing the data of customers should be the number one priority for any business. Without customers, the business would fail. And without data security, the customers will take their business to a competing company. In today's world-wide economy, customers have many choices of companies to do business with. Securing customer data keeps customers happy (Nutt, 2007).

2.1.4.2. Product Information

Productivity is also a driver, which does not get the attention of the press but is important to organizations nonetheless. Loss of important data lowers overall productivity, as employees have to deal with time-consuming customer issues without the aid of computer databases. Data loss also results in application failures and similar system problems, making it difficult for people to do their jobs. A poor data protection strategy may leave people waiting for long periods of time for systems to be restored after a failure. During that time, employees may be idle or able to work only in a reduced capacity, further diminishing productivity (Petrocelli, 2005).

In addition for many industries, protecting information about new and existing products is also a priority. Competing companies may be looking for a leg up and could find that help by using stolen data. Innovation is key to surviving in most businesses, and in order to protect its intellectual property, a company needs to pay attention to security of data on their products (Mayock, 2010; Nutt, 2007).

2.1.4.3. Employee information

Most companies have detailed personal information about employees, such as Social Security Numbers, addresses, telephone numbers, and employment records. It's vital to the success of a business to protect the interests of its employees. Employees contribute greatly to the success of a company and their satisfaction at workplace is key to this achievement (Nutt, 2007).

2.1.4.5 Company information

It is important for many companies to protect financial information and other data about the business. If accessible to unauthorized users, this information could harm the business's reputation or provide impetus for legal action against the company. Protecting company information is therefore essential (Nutt, 2007).

2.2 Cybercrimes

Saini, Rao and Panda (2012) categorized cybercrimes into four categories which include: data crimes, network crimes, access crimes, aiding and abetting.

2.2.1. Definition of Cybercrime

Cybercrime is a subcategory of computer crime and it refers to criminal offenses committed using the internet or another computer network as a component of the crime (Shinder, 2002). Schell (2004) defined cybercrime as a crime related to technology, computers and the internet and it concerns governments, industries and citizens worldwide where cybercrime takes the form of either piracy, phreaking (obtaining free telephone calls), cyber stalking, cyber terrorism and cyber pornography. Milhorn, (2007) on the other hand, simply defines cybercrime as any

activity that uses the internet to commit a crime. Cybercrime can also be defined broadly as any activity on the internet that offends human sensibilities (Dugal n.d).

2.2.2 Cybercrime Differentiated from Traditional Crime

Cybercrimes, are uniquely different from traditional crimes and they are often harder to detect and prosecute. The Swedish Emergency Management Agency's 2008 report, "Information Security in Sweden: Situational Assessment," observes that criminal activity on the Internet has become progressively more sophisticated. Perpetrators carry out cybercrimes through small, targeted Internet attacks, as well as launching significant attacks using large networks of commercially leased, hijacked computers.

, while researching on the legal issues of cybercrime in China, Chen Junjiing (Glenn et al, 2009) concluded that these crimes are more widespread than traditional crimes and are increasing at a faster rate. Furthermore, cybercrime does greater damage to society than traditional crime and is more difficult to investigate. In her study of the use of cybercrime for fraudulent financial activity in France, Vanessa Vitaline (Glenn et al, 2009 pg 88-93), identifies typical characteristics of cybercrime: it is inexpensive, fast, anonymous, and has global impact. Its perpetrators use remote intervention to carry out their crimes, recruiting experts in data processing and networking to assist them in activities designed to corrupt computer systems.

2.2.3 Data/Information Crimes

These crimes mainly target data/information. The first one is data interception where an attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the data collected may be the end goal of the attack. This attack usually involves sniffing

network traffic, but may include observing other types of data streams, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted (Saini, Rao and Panda 2012). However, in all variants of this attack, and distinguishing this attack from other data collection methods, the attacker is not the intended recipient of the data stream. Unlike some other data leakage attacks, the attacker is observing explicit data channels (e.g. network traffic) and reading the content. This differs from attacks that collect more qualitative information, such as communication volume, not explicitly communicated via a data stream (CAPEC, 2010).

The second one includes data modification. Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites. In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it. An example of this is changing the dollar amount of a credit card transaction/bank from $100 to say $10,000. In a replay attack, an entire set of valid data is repeatedly interjected onto the network. An example would be to repeat, one thousand times, a valid $100 bank account transfer transaction (Oracle, 2003).

The third is data theft which is used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information is

apprehended, it is likely he or she will be prosecuted to the fullest extent of the law (Saini, Rao & Panda 2012).

2.2.4 Network Crimes

These crimes are aimed at compromising or bringing down the communication infrastructure and network of a business. These crimes can be divided into two categories that are network interference and network sabotage (Tittel, Chapple, & Stewart, 2003).

Network interference includes any action that Interferes with the functioning of a computer Network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing Network data. Network sabotage on the other hand deals with the intentional and premeditated attacks on a company's or institutional network to either temporarily disable it or completely destroy it making it inoperable. This could be achieved by attacks centered on a company's internet hardware and software or the infrastructure the company depends on i.e. fiber optic cables (DSL Reports, 2011).

2.2.5 Access Crimes

System Malware dissemination includes crimes that involves all the malicious software that attaches itself to other software and includes but not limited to virus, worms, time bombs, logic bombs, among many others are examples of malicious software that destroys the system of the victim (Saini, Rao & Panda 2012).

2.2.6 Aiding and abetting cyber crimes

There are three elements to most aiding and abetting charges against an individual. The first is that another person has committed the crime. Second, the individual being charged had knowledge of the crime or the principals' intent. Third, the individual

provided some form of assistance to the principal. An accessory in legal terms is typically defined as a person who assists in the commission of a crime committed by another or others. In most cases, a person charged with aiding and abetting or accessory has knowledge of the crime either before or after its occurrence (Leagal Info, 2009). A person who is aware of a crime before it occurs, and who gives some form of aid to those committing the crime, is known in legal terms as an "accessory before the fact." He or she may assist through advice, actions, or monetary support. A person who is unaware of the crime before it takes place, but who helps in the aftermath of the crime, is referred to as an "accessory after the fact" (Saini, Rao & Panda 2012).

2.3 Security Framework and Policy

Hospitality businesses should have a comprehensive security framework implemented, updated and monitored and evaluated to curb cybercrime incidences (Kevin, 2011). The policy should include the use of anti-malware programs and firewall system, information encryption and communication encryption, password management systems, network security system and establishments physical security that promotes information security (Tittel, Chapple, & Stewart, 2003).

2.3.1 Accountability and access control policies

Access controls are necessary to protect the *confidentiality, integrity,* and *availability* of objects (and by extension their information and data). The term *access control* is used to describe a broad range of controls, from forcing a user to provide a valid username and *password* to log on to preventing users from gaining access to a resource outside of their sphere of access (Jatinder & Sushil, 2009).

2.3.1.1 Access controls

Access controls can be divided into three categories. The first category is preventative access control which is deployed to stop unwanted or unauthorized activity from occurring. Examples of preventative access controls include fences, security policies, security awareness training, and antivirus software (Tittel, Chapple, & Stewart, 2003).

Secondly is detective access control which is deployed to discover unwanted or unauthorized activity. Examples of detective access controls include security guards, supervising users, incident investigations, and intrusion detection systems. (Tittel, Chapple & Stewart, 2003).

Thirdly is corrective access control which is deployed to restore systems to normal after an unwanted or unauthorized activity has occurred. Examples of corrective access controls include alarms, mantraps, and security policies (Tittel, Chapple, & Stewart, 2003).

2.3.1.2 Implementation of access control

The implementation of an access control can be categorized as administrative, logical/technical, or physical. Administrative access controls are the policies and procedures defined by an organization's security policy to implement and enforce overall access control. Examples of administrative access controls include policies, procedures, hiring practices, background checks, data classification, security training, vacation history, reviews, work supervision, personnel controls, and testing (Harold & Micki, 2007).

Logical access controls and technical access controls are the hardware or software mechanisms used to manage access to resources and systems and provide protection

for those resources and systems. Examples of logical or technical access controls include encryption, smart cards, passwords, biometrics, constrained interfaces; access control lists (ACLs), protocols, firewalls, routers, intrusion detection systems, and clipping levels (Harold & Micki, 2007).

Physical access controls are the physical barriers deployed to prevent direct contact with systems. Examples of physical access controls include guards, fences, motion detectors, locked doors, sealed windows, lights, cable protection, laptop locks, swipe cards, dogs, video cameras, mantraps, and alarms (Tittel, Chapple, & Stewart, 2003).

2.3.1.3 Access controls

Access controls govern a subject's access to objects. The first step in this process is identifying the subject. In fact, there are several steps preceding actual object access: identification, authentication, authorization, and accountability.

Identification is the process by which a subject professes an identity and accountability is initiated. A user providing a username, a logon ID, a personal identification number (PIN), or a smart card represents the identification process. Providing a process ID number also represents the identification process. Once a subject has identified itself, the identity is accountable for any further actions by that subject. Information Technology (IT) systems track activity by identities, not by the subjects themselves. A computer doesn't know one human from another, but it does know that your user account is different from all other user accounts (Hancock, 2002).

Authentication is the process of verifying or testing that the claimed identity is valid. Authentication requires that the subject provide additional information that must exactly correspond to the identity indicated. The most common form of authentication

is a password. However, there are at least three other types of information that can be used for authentication: A Type 1 authentication factor is something you know, such as a password, personal identification number (PIN), lock combination, pass phrase, mother's maiden name, favorite color, and so on; A Type 2 authentication factor is something you have, such as a smart card, token device, memory card, and so on. This can also include your physical location, referred to as the "somewhere you are" factor; A Type 3 authentication factor is something you are, such as fingerprints, voice print, retina pattern, iris pattern, face shape, palm topology, hand geometry, and so on (Tittel, Chapple, & Stewart, 2003). However, once a subject is authenticated, their access must be authorized. The process of authorization ensures that the requested activity or object access is possible given the rights and privileges assigned to the authenticated identity. In most cases, the system evaluates an access control matrix that compares the subject, the object, and the intended activity. If the specific action is allowed, the subject is authorized. If the specific action is not allowed, the subject is not authorized (Ekaterina, 2010).

An organization's security policy can only be properly enforced if accountability is maintained. In other words, security can only be maintained if subjects are held accountable for their actions. Effective accountability relies upon the capability to prove a subject's identity and track their activities. Thus, accountability builds on the concepts of identification, authentication, authorization, access control, and auditing.

2.3.1.4 Identification and authentication techniques

Identification and authentication are always together as a single two-step process. Providing an identity is step one and providing the authentication factor(s) is step two. Without both, a subject cannot gain access to a system neither element alone is useful.

Some of the identification and authentication techniques are discussed below (Goudie, 2011).

Passwords are the most commonly used authentication technique is the use of keywords, but they are also considered to be the weakest form of protection. Passwords are poor security mechanisms for several reasons which include: users typically choose passwords that are easy to remember, and therefore easy to guess or crack; Randomly generated passwords are hard to remember, thus many users write them down; Passwords are easily shared, written down, and forgotten; Passwords can be stolen through many means, including observation, recording and playback, and security database theft; Passwords are often transmitted in clear text or with easily broken encryption protocols; Password databases are often stored in publicly accessible online locations; Short passwords can be discovered quickly in brute force attacks. Passwords can be effective if selected intelligently and managed properly. There are two types of passwords: static and dynamic. Static passwords always remain the same. Dynamic passwords change after a specified interval of time or use (Harold & Micki 2007).

Biometrics factor is a behavioral or physiological characteristic that is unique to a subject. There are many types of biometric factors, including fingerprints, face scans, iris scans, retina scan, palm scan (also known as palm topography or palm geography), heart/pulse pattern, voice pattern, signature dynamics, keystroke patterns, and so on. Biometrics can be used as an identifying or authentication technique. The use of biometrics promises universally unique identification for every person on the planet (Burgess & Power 2008).

Tokens are password-generating devices that subjects must carry with them. Token devices are a form of "something you have." A token can be a static password device, such as an ATM card. To use an ATM card, you must supply the token (the ATM card itself) and your PIN (Tittel, Chapple, & Stewart, 2003).

Tickets authentication is a mechanism that employs a third-party entity to prove identification and provide authentication. The most common and well-known ticket system is *Kerberos*. Kerberos was developed under Project Athena at MIT. The Kerberos authentication mechanism centers on a trusted server (or servers) that host the functions of the Key Distribution Center (KDC), the Ticket Granting Service (TGS), and the Authentication Service (AS). Kerberos uses symmetric key cryptography to authenticate clients to servers. All clients and servers are registered with the KDC, so it maintains the secret keys of all network members (Harold & Micki 2007).

2.3.1.5 Access Control Techniques

Once a subject has been identified and authenticated and accountability has been established, they must be authorized to access resources or perform actions. Authorization can occur only after the subject's identity has been verified through authentication. Systems provide authorization through the use of access controls. Access controls manage the type and extent of access subjects have to objects. Many access control models have been developed and including the following: State machine model, Bell-LaPadula, Biba, Clark-Wilson, Information flow model, Non-interference model, Take-Grant model and Access control matrix (Tittel, Chapple, & Stewart, 2003).

2.3.1.6 Access control administration

Access Control Administration is the collection of tasks and duties assigned to an administrator to manage user accounts, access, and accountability. A system's security is based on effective administration of access controls. Remember that access controls rely upon four principles: identification, authentication, authorization, and accountability. In relation to access control administration, these principles transform into three main responsibilities: User account management, activity tracking, access rights and permissions management (Hancock, 2002).

2.3.2 Attack monitoring

Monitoring is the programmatic means by which subjects are held accountable for their actions while authenticated on a system. Monitoring is also the process by which unauthorized or abnormal activities are detected on a system. Monitoring is necessary to detect malicious actions by subjects, as well as attempted intrusions and system failures. It can help reconstruct events, provide evidence for prosecution, and produce problem reports and analysis. Auditing and logging are usually native features of an operating system and most applications and services. Thus, configuring the system to record information about specific types of events is fairly straightforward (Tittel, Chapple, & Stewart, 2003).

2.3.2.1 Intrusion detection

An intrusion detection system (IDS) is a product that automates the inspection of audit logs and real-time system events. IDSs are primarily used to detect intrusion attempts, but they can also be employed to detect system failures or rate overall performance. IDSs watch for violations of confidentiality, integrity, and availability.

Attacks recognized by IDS can come from external connections (such as the Internet or partner networks), malicious code, trusted internal subjects attempting to perform unauthorized activities, and unauthorized access attempts from trusted locations (Wil, 2009).

An IDS can actively watch for suspicious activity, peruse audit logs, send alerts to administrators when specific events are discovered, lock down important system files or capabilities, track slow and fast intrusion attempts, highlight vulnerabilities, identify the intrusion's origination point, track down the logical or physical location of the perpetrator, terminate or interrupt attacks or intrusion attempts, and reconfigure routers and firewalls to prevent repeats of discovered attacks (John, 2009).

Intrusion prevention requires adequate maintenance of overall system security, such as applying patches and setting security controls. It also involves responding to intrusions discovered via IDS by erecting barriers to prevent future repeats of the same attack. This could be as simple as updating software or reconfiguring access controls, or it could be as drastic as reconfiguring a firewall, removing or replacing an application or service, or redesigning an entire network (Tittel, Chapple, & Stewart, 2003).

2.3.3 Network security

Communication systems are vulnerable to attacks in much the same way any other aspect of the IT infrastructure is vulnerable. Understanding the threats and the possible countermeasures is an important part of securing an environment. Any activity or condition that can cause harm to data, resources, or personnel must be addressed and mitigated if possible. Keep in mind that harm includes more than just destruction or damage; it also includes disclosure, access delay, denial of access,

fraud, resource waste, resource abuse, and loss. Common threats against communication systems security include denial of service, eavesdropping, impersonation, replay, and modification (Thomas, Justin & John 2005).

2.3.4 Data/Information storage policies

Because Data is also processed through a computer's storage resources - both memory and physical media, precautions must be in place to ensure that these basic resources are protected against security vulnerabilities as well. Organizations should use several types of storage to maintain systems and user data. A balance between the various storage types should be struck in order to satisfy an organization's computing requirements. There are a variety of data storage techniques and media available in the market today and an organization should choose a variety for backing up their data (Warren, Jennifer, & Daniel, 2009).

Backing up critical information is a key part of maintaining the availability and integrity of data. Systems fail for various reasons, such as hardware failure, physical damage, software corruption, and malicious destruction from intrusions and attacks. Having a reliable backup is the best form of insurance that the data on the affected system is not permanently lost (John, 2009).

2.4 Executive management support in fighting cybercrimes

Any information security group is incapacitated or at best semi functional if there is no executive management support. Management support must be clearly and entirely communicated to all employees, empowering the group tasked to protect the critical information assets of the enterprise. Such management support is especially important and critical to allow the information security group to assign ownership of security

areas and risks. Individuals and/or groups may from time to time attempt to brush aside any responsibility or ownership for addressing security risks (Thomas, Justin, & John, 2005).

However, without timely assignment of security risks for remediation or area ownership to support the risk assessment process, the company is once again placed at increased risk. The information security group can play a key role in educating management regarding security risks and group's function, however, management must be open minded and willing to listen. Most often and unfortunately, management suddenly places importance on information protection after a major security breach, especially when speaking to the public and reporters, however, this reactionary behavior is temporary and ineffective in managing security risks due to lack of serious and sustained management commitment to the protection of corporate information assets (Bragg, 2002).

Management of an organization is an important aspect in the maintaining security of information within their businesses. This is because they control the resources that are needed by the IT department such as manpower recruitment, budget allocation and approval, policy implementation, infrastructure development among many others (Tittel, Chapple, & Stewart, 2003).

2.4.1 Employee employment and termination

Humans are the weakest element in any security solution. No matter what physical or logical controls are deployed, humans can discover ways to avoid the controls, circumvent or subvert the controls, or disable the controls. Thus, it is important to take into account the humanity of your users when designing and deploying security solutions for your environment (Tittel, Chapple, & Stewart, 2003).

Hiring new staff typically involves several distinct steps: defining a job description, setting a classification for the job, screening candidates, and hiring and training the one best suited for the job. Any job description for any position within an organization should address relevant security issues. In a detailed job description, a comparison is made between what a person should be responsible for and what they actually are responsible for. Managers should audit privilege assignments to ensure that workers do not obtain access that is not strictly required for them to accomplish their work tasks (Ekaterina, 2010).

Screening candidates for a specific position is based on the sensitivity of the position and is defined by the job description. The sensitivity and classification of a position is dependent upon the level of harm that could be caused by accidental or intentional violations of security by a person in a specific job position. Thus, the thoroughness of the screening process should reflect the security of the position to be filled (Bragg, 2002).

Background checks and security clearances are essential elements in proving that a candidate is adequate, qualified, and trustworthy for a secured position. Background checks include obtaining a candidate's work and educational history; checking references; interviewing colleagues, neighbors, and friends; checking police and government records for arrests or illegal activities; verifying identity through fingerprints, driver's license, and birth certificate; and holding a personal interview. This process could also include a polygraph test, drug testing, and personality testing/evaluation (Tittel, Chapple, & Stewart, 2003).

When a new employee is hired, they should sign an employment agreement. Such a document outlines the rules and restrictions of the organization, the security policy,

the acceptable use and activities policies, details of the job description, violations and consequences, and the length of time the position is to be filled by the employee (John, 2009).

Another important document is a Non-Disclosure Agreement (NDA). An NDA is used to protect the confidential information within an organization from being disclosed by a former employee. When a person signs an NDA, they agree not to disclose any information that is defined as confidential to anyone outside of the organization. Violations of an NDA are often met with strict penalties (Hancock, 2002).

When an employee must be terminated, there are numerous issues that must be addressed. A termination procedure policy is essential to maintaining a secure environment even in the face of a disgruntled employee who must be removed from the organization. The reactions of terminated employees can range from understanding acceptance to violent, destructive rage. A sensible procedure for handling terminations must be designed and implemented to reduce incidents (Tittel, Chapple, & Stewart, 2003).

The termination of an employee should be handled in a private and respectful manner. However, this does not mean that precautions should not be taken. Terminations should take place with at least one witness, preferably a higher-level manager and/or a security guard. Once the employee has been informed of their release, they should be escorted off the premises immediately. Before the employee is released, all organization-specific identification, access, or security badges as well as cards, keys, and access tokens should be collected (Tittel, Chapple, & Stewart, 2003).

An exit interview should be performed. However, this typically depends upon the mental state of the employee upon release and numerous other factors. If an exit interview is infeasible immediately upon termination, it should be conducted as soon as possible. The primary purpose of the exit interview is to review the liabilities and restrictions placed on the former employee based on the employment agreement, nondisclosure agreement, and any other security-related documentation (Hancock, 2002).

Some other issues that should be handled as soon as possible once the tenure of the employee has been terminated: Making sure the employee returns any organizational equipment or supplies from their vehicle or home, remove or disable the employee's network user account, notify human resources to issue a final paycheck, pay any unused vacation time, and terminate benefit coverage, arrange for a member of the security department to accompany the released employee while they gather their personal belongings from the work area (Bragg, 2002).

In most cases, the business should disable or remove an employee's system access at the same time or just before they are notified of being terminated. This is especially true if that employee is capable of accessing confidential data or has the expertise or access to alter or damage data or services. Failing to restrict released employees' activities can leave your organization open to a wide range of vulnerabilities, including theft and destruction of both physical property and logical data (John, 2009).

2.4.2 IT budgeting

Inadequate budgets may be the consequence of insufficient or inexistent executive management support or lack of priority placed upon the information security function.

In order to properly budget for the protection of the enterprise information assets, information security priority, and management support backed by solid financial contribution must first exist. Absence of reasonable financial support may lead to an incapacitated information security function that looks good on the organization chart for the regulators and stockholders, but which is unable to execute the required plan to reduce the information security risks. Inadequate security budgets ultimately lead to higher security risks, an ineffective and inefficient information security group, an uneducated and unaware enterprise, inadequate information security staff levels, and unqualified information security professionals due to lower salaries and unavailable quality information security training (Burgess & Power, 2008).

The IT department should be allocated a budget that is adequate to run and maintain the security measures in the organization. There are a variety of costs that are incurred apart from remuneration of the employees in the IT and security. These costs include the cost of purchase, development and licensing of the security solutions, the cost of implementation and customization, the cost of annual operations, maintenance, administration etc., the annual cost of repairs and upgrades, productivity improvement or loss, cost of changes to environment and the cost of testing and evaluation (Tittel, Chapple, & Stewart, 2003).

2.4.3 Security awareness training

The successful implementation of a security solution requires changes in user behavior. These changes primarily consist of alterations in normal work activities to comply with the standards, guidelines, and procedures mandated by the security policy. Behavior modification involves some level of learning on the part of the user.

There are three commonly recognized learning levels: awareness, training, and education (Bacik, 2008).

Awareness is considered a prerequisite to actual training. The goal of creating awareness is to bring security into the forefront and make it a recognized entity for users. Awareness is not created through a classroom type of exercise but rather through the work environment. There are many tools that can be used to create awareness, such as posters, notices, newsletter articles, screen savers, T-shirts, rally speeches by managers, announcements, presentations, mouse pads, office supplies, memos, and so on (Burgess & Power, 2008).

Training is teaching employees to perform their work tasks and to comply with the security policy. All new employees require some level of training so they will be able to comply with all standards, guidelines, and procedures mandated by the security policy. New users need to know how to use the IT infrastructure, where data is stored, and how and why resources are classified (Burgess & Power, 2008).

Education is a more detailed endeavor in which students/users learn much more than they actually need to know to perform their work tasks. Education is most often associated with users pursuing certification or seeking job promotion. It is typically a requirement for personnel seeking security professional positions. A security professional requires extensive knowledge of security and the local environment for the entire organization and not just their specific work tasks (Philip, 2008).

2.5 Impacts of cyber-crime

Organized crime groups are using the Internet for major fraud and theft activities. There are trends indicating organized crime involvement in white-collar crime. As

criminals move away from traditional methods, internet-based crime is becoming more prevalent. Internet-based stock fraud has earned criminals millions per year leading to loss to investors, making it a lucrative area for such crime (Saini, Rao & Panda, 2012).

2.5.1 Potential economic impact

The 2011 Norton Cybercrime disclosed that over 74 million people in the United States were victims of cybercrime in 2010. These criminal acts resulted in $32 billion in direct financial losses. Further analysis of this growing problem found that 69 percent of adults that are online have been victims of cybercrime resulting in 1 million cybercrime victims a day. Many people have the attitude that cybercrime is a fact of doing business online! (Kevin, 2011).

As today‘s consumer has become increasingly dependent on computers, networks, and the information these are used to store and preserve, the risk of being subjected to cyber-crime is high. Some of the surveys conducted in the past have indicated as many as 80% of the companies’ surveyed acknowledged financial losses due to computer breaches. The approximate number impacted was $450 million. Almost 10% reported financial fraud (PTI, 2009). Each week we hear of new attacks on the confidentiality, integrity, and availability of computer systems. This could range from the theft of personally identifiable information to denial of service attacks.

As the Kenyan economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy (Kevin, 2011).

The disruption of international financial markets could be one of the big impacts and remains a serious concern. The modern economy spans multiple countries and time zones. Such interdependence of the world's economic system means that a disruption in one region of the world will have ripple effects in other regions. Hence any disruption of these systems would send shock waves outside of the market which is the source of the problem (Ekaterina, 2010).

Productivity is also at risk. Attacks from worms, viruses, etc. take productive time away from the user. Machines could perform more slowly; servers might be in accessible, networks might be jammed, and so on. Such instances of attacks affect the overall productivity of the user and the organization. It has customer service impacts as well, where the external customer sees it as a negative aspect of the organization (Ekaterina, 2010).

In addition, user concern over potential fraud prevents a substantial cross-section of online shoppers from transacting business. It is clear that a considerable portion of e-commerce revenue is lost due to shopper hesitation, doubt, and worry. These types of consumer trust issues could have serious repercussions for businesses (Saini, Rao & Panda, 2012).

2.5.2 Impact on market value

The economic impact of security breaches is of interest to companies trying to decide where to place their information security budget as well as for insurance companies' that provide cyber-risk policies (Gordon et al 2003). In assessing economic impact of security breaches, damage is not restricted to physical destruction or harm of computer circuitry but includes loss of use and functionality (Ariz, 2000). This new and evolving view of damage becomes even more important as many firms rely on

information systems in general and the Internet in particular to conduct their business. As the characteristics of security breaches change, companies continually reassess their IS environment for threats (Kelly, 1999).

Depending on the size of the company, a comprehensive assessment of every aspect of the IS environment may be too costly and impractical. IS risk assessment provides a means for identifying threats to security and evaluating their severity. Risk assessment is a process of choosing controls based on the probabilities of loss. In Information Security, risk assessment addresses the questions of what is the impact of an IS security breach and how much will it cost the organization (Kelly, 1999). However, assessing the financial loss from a potential IS security breach is a difficult step in the risk assessment process for the following reasons: Many organizations are unable or unwilling to quantify their financial losses due to security breaches (Power, 2001) therefore the lack of historical data on cybercrimes. Many security breaches are unreported. Companies are reluctant to disclose these breaches due to management embarrassment, fear of future crimes and fear of negative publicity (Power, 2001). Companies are also wary of competitors exploiting these attacks to gain competitive advantage (Power, 2001). Additionally, companies maybe fearful of negative financial consequences resulting from public disclosure of a security breach. Previous research suggests that public news of an event that is generally seen as negative will cause a drop in the firm‘s stock price (Saini, Rao & Panda, 2012).

In addition, potential intangible losses such as loss of competitive advantage that result from the breach and loss of reputation (D‘Amico, 2000) are not included because intangible costs are not directly measurable.

A market value approach captures the capital market‘s expectations of losses resulting from the security breach. This approach is justifiable because often companies are impacted more by the public relations exposure than by the attack itself (Hancock, 2002). Moreover, managers aim to maximize a firm‘s market value by investing in projects that either increase shareholder value or minimize the risk of loss of shareholder value. Therefore, in this study we elected to use market value as a measure of the economic impact of security breach announcements on companies. In the following section we define a security breach as an unexpected event and discuss the characteristics of DDoS attacks (Saini, Rao & Panda, 2012).

2.5.3 Impact on consumer trust

Since cyber-attackers intrude into others‘ space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site on a long term basis. The site in question is termed as the fraudulent, while the criminal masterminding the hidden attack is not recognized as the root cause. This makes the customer lose confidence in the said site and in the internet and its strengths (Ekaterina, 2010).

According to reports sponsored by the Better Business Bureau Online, over 80% of online shoppers cited security as a primary worry when conducting business over the Internet. About 75% of online shoppers terminate an online transaction when asked for the credit card information. The perception that the Internet is rife with credit card fraud and security hazards is growing. This has been a serious problem for e-commerce (Burgess & Power, 2008).

Complicating the matter, consumer perceptions of fraud assess the state to be worse than it actually is. Consumer perception can be just as powerful - or damaging - as

fact. Hence users' concerns over fraud prevent many online shoppers from transacting business. Concern over the credibility of an e-business in terms of being unsafe or cluttered makes a shopper reluctant to transact business. Even the slightest perception of security risk or amateurish commerce seriously jeopardizes potential business (Saini, Rao & Panda, 2012).

2.6 Why hotels are easy targets.

Identity theft (a form of cybercrime) is a growing concern for hospitality providers because every hotel, resort, casino or restaurant offers the elements necessary for a successful attack. These elements include motive, access and low risk as explained in the following sections.

2.6.1 Motive.

Many hospitality workers have high-turnover and working in close proximity to guests of higher economic means.

2.6.2 Access.

Travelers often carry important financial documents. They often fail to protect their property, leaving credit cards and sensitive business information on the desk or in the room safe. They access hotel business centers that may be compromised by keystroke loggers that steal passwords and credit card numbers, and they use Ethernets that may have inadequate security controls. Guests regularly give their credit card information over the Internet, by phone and in person. This data often is stored in databases easily accessed by employees whose criminal backgrounds may not have been checked prior to hiring. In addition to these internal threats, hospitality companies are vulnerable to

external attacks, in which a hacker breaks into billing and reservation systems to steal customer information.

2.6.3 Low risk.

Since many hospitality chains rarely track computer system users, they usually cannot discover, investigate and prosecute identity thieves.

2.7 Theoretical model for the study

This study will adopt a Data Centric Security Model (DCSM) developed by an IBM team to secure data in the organization through a variety of layers of security. This model places data at the core because information assets are the drivers of today's organizations. This is because information represents the companies know how, critical business processes are driven by information and companies relationships trust are maintained by an informational exchange (Bilger, et al. 2007).

DCSM allows the link between IT security technology and business strategy objectives by linking security services to the data that needs protection. The data being handled is classified and access control policies governing data use are implemented. The most important aspect of DCSM is that it does not specifically depend explicitly on specific security products and technologies and is independent of the underlying security infrastructure (Bilger, et al. 2007).

Bilger, et al. (2007) says DCSM first objective is to identify the owner of data, be it individual, customer or a business line. Requirements for data handling of each type of data are gathered as this will help in the development of policies for each of the data. DCSM is composed of two pillars that is the data pillar and policy pillar. The policy pillar represented by the second inner circle from the center summarized the

business requirements and regulations required in handling data. The third circle utilizes the security and business requirements to define classification of data that is the Business Data Classification (BDC) that give the data attributes and ownership, location and origin time. Data Control Rules (DCRs) are established based on the BDC and are used to establish policies and practices granting appropriate access to support corporate data handling policies which is presented by the second last layer. The outer layer presents the security perimeter defense, data protection while at rest, or even encapsulation of data during transmission (Bilger, et al. 2007).

The DCSM model will be used as the basis of analyzing the information security measures taken by the hotels by looking at the various aspects of the model from the classification and storage of data and information, the controls put in place for people accessing the information and authentications and privileges each has to manipulate the information, the physical and software securities put in place to prevent unauthorized access of information.

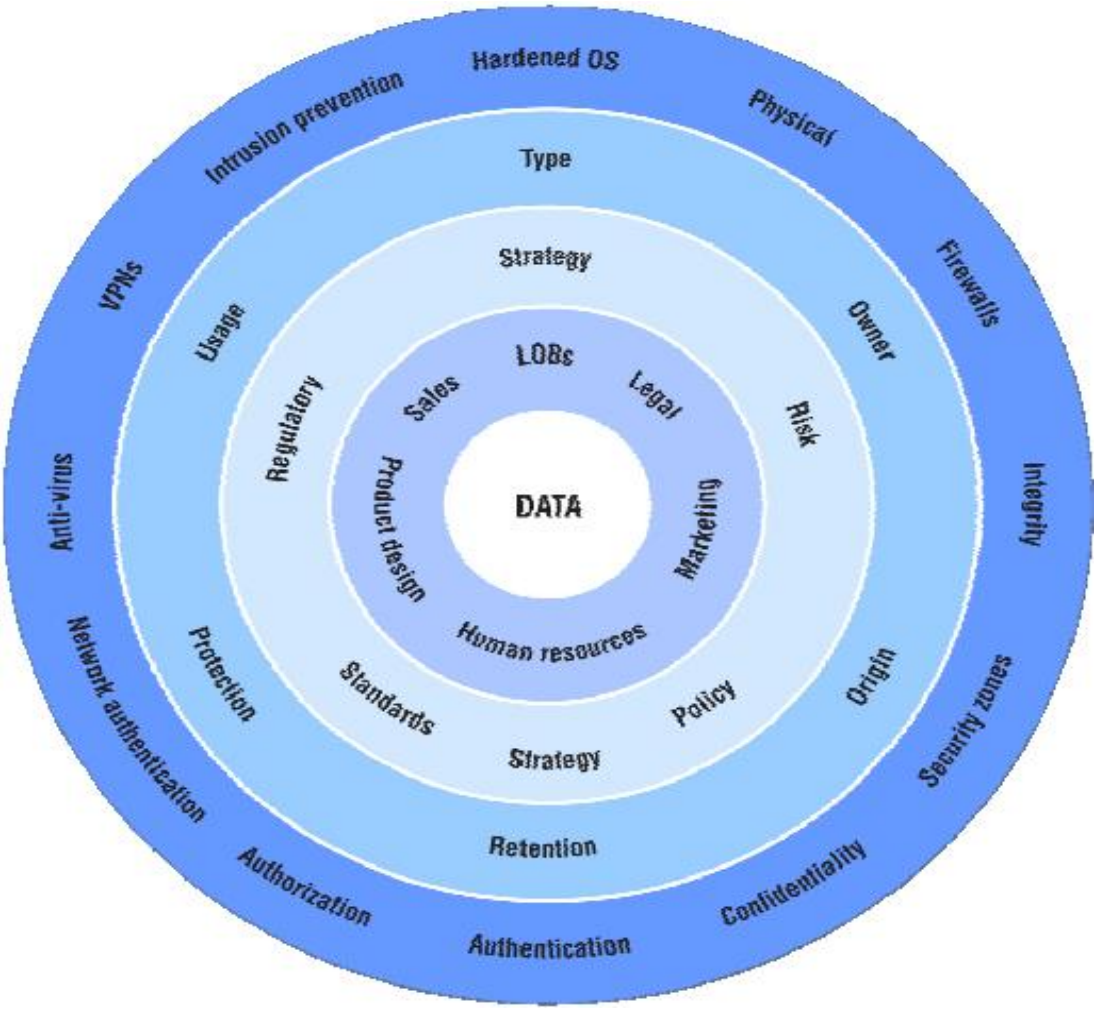

Figure 2. 2: Data Centric Security Model

Source: (Bilger, et al. 2007).

2.8 Conceptual framework for the study

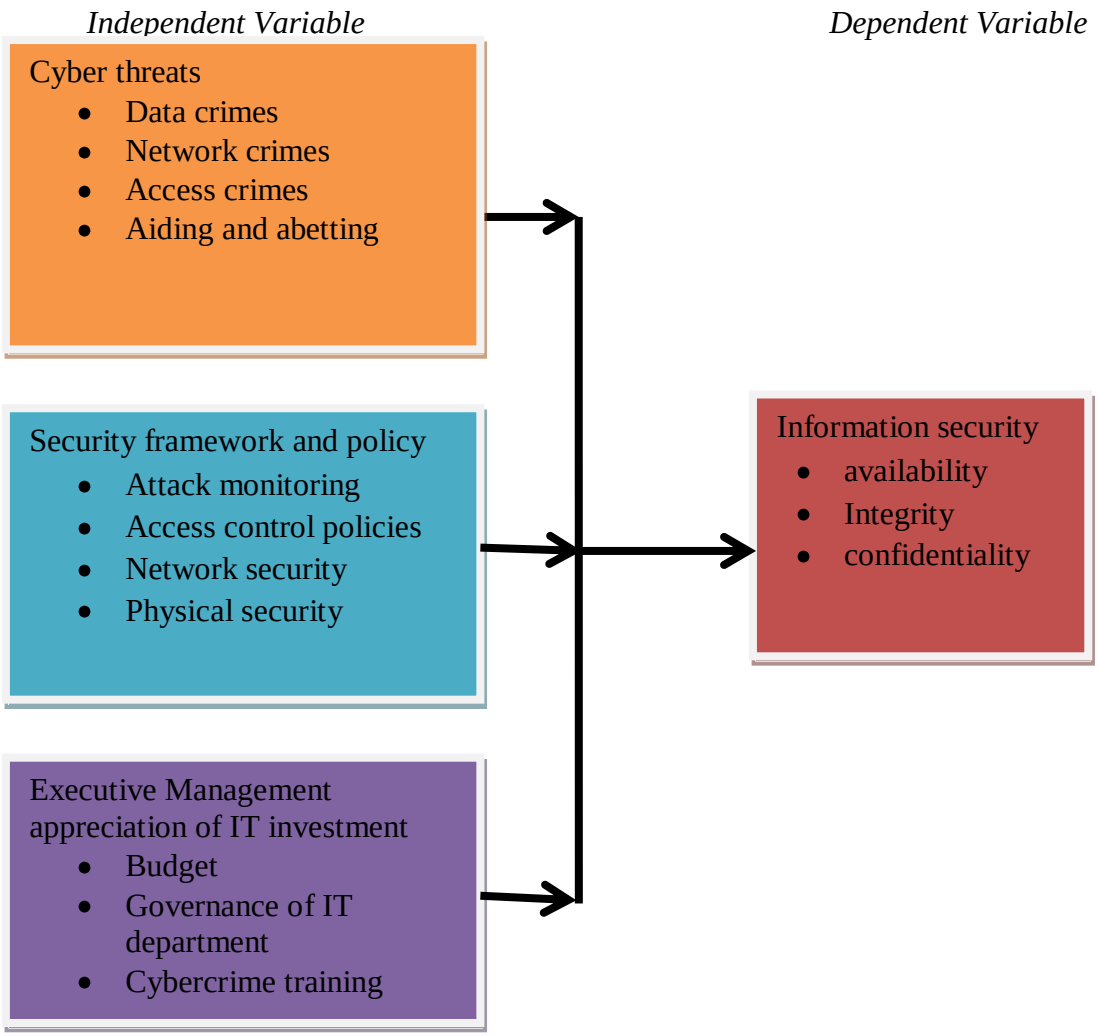

Figure 2. 3 Conceptual framework

Source: *Adopted and modified from the DCSM model, 2013*

The researcher conceptualized cybercrime management which was the independent variable to be cyber-threat, security framework policies and management appreciation of IT investments. Cyber threats were divided into data crimes, network crimes, access crimes, and aiding and abetting. Security framework policies included attack monitoring, access control policies, network security protocols and physical security. Executive management appreciation of IT investment included budgets, governance of the IT department and training on cybercrimes. The dependent variable which was

information security was conceptualized to include information availability, integrity and confidentiality.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

Chapter two reviewed literature on cybercrime and its effects, the importance of information security and the various ways of ensuring optimal information security. In this chapter, the research methodology which was used in attempt to achieve the objectives of the study as explained. It outlines the procedures used to gather information, the study area, research design, sample size, sampling technique, research instruments to be used, validity and reliability, data analysis and presentation.

3.1 Study Area

The research was carried out in selected hotel establishments in Nairobi city. Nairobi is the capital and largest city in Kenya. Nairobi city was among the earliest adopters of Internet as most of the import and export businesses, industries and overseas clients and the academic sector during the period of 1990 to 1998. The key challenge of this period was the limited and high cost of international bandwidth; the high cost of both dial-up and domestic leased lines; the limited penetration of the PCs; the lack of policy and regulatory environment ; and the lack of appropriate IT skills (Njoroge, 2009 Magutu 2011). From 1999 to 2004, the Kenyan government restructured the communication sector with the aim of introducing competition and paving way for the private sector participation. This resulted in the formation of a regulator of the independent ICT sector and thus Communication Commission of Kenya (CCK) now Communication Authority of Kenya (CAK) whose mandate was to spearhead sector

reforms. The elapse of the Telkom Kenya's exclusivity in June 2004 in the provision of various services including internet bandwidth marked the grand phase of internet development in Kenya (Magutu, Ondimu, & Ipu, 2011).

CAK expanded the competition in cellular mobile telecommunications market and this resulted in a range of innovative products and services such as Mpesa. as a result of this new wave of reforms coupled by the increased penetration of PCs and the level of IT skills, the number of regular internet users increased to over 3 million out of a population of about 35 million (Magutu, Ondimu, & Ipu, 2011).

The development of national broadband fiber optic connectivity to take advantage of the three submarine cables that landed in the coastal city of Mombasa lowered the cost of internet access and thus spread the digital dividends to a bigger proportion of Kenyans. Magutu Ondimu, & Ipu (2011) projected that by the year 2013, the internet penetration in Kenya should be close to 50 percent due to the provision of 3G mobile internet services at very competitive prices and the adoption of the unified licensing regime.

Due to the increasing competition in the hospitality sector hotel businesses have increasingly adopted ICT technology as a strategic positioning tools. Modern technology has been employed to improve the customer experience and also the business process to ensure efficiency and reliability. This has seen adoption of technologies such as high speed internet connectivity, Wi-Fi internet, property management systems, and electronic door lock systems among other technologies.

3.2 Research Design

The research design is the general plan of how a researcher will go about answering their research questions. Kothari (2004) says that research design is the conceptual structure within which a research is conducted and constitutes the blueprint for data collection measurement and analysis.

The research employed explanatory research design as it enables one to analyze data quantitatively and to further subject the data to inferential statistics (Saunders, Lewis & Thornhill, 2009). The researcher used this design to investigate and understand cybercrime effects on information security of hotels in Nairobi by subjecting the data from the field to statistical tests for correlation between the independent variable (cybercrime) to the dependent variable (information security).

3.3 Target Population

The target population involved employees in the IT department of the targeted hotels and also the employees in the front office departments, supplies, finance department and management of the chosen hotels which was 935.

3.4 Sampling Design

This section looked at the sampling technique, sampling framework, the sample size determination and distribution as detailed in section 3.4.1 to 3.4.2.

3.4.1 Sampling Technique

Purposive sampling was used to select four hotels in Nairobi that fulfilled the criteria of; early adopters of ICT, have utilized the internet platform to transact hotel business for example online booking. This was because they had the required information that

would answer the objectives of the study and would have at least experienced forms of cybercrimes against their organizations. Stratified sampling was used to divide the each hotel into departments. Also the employees were stratified into management (departmental managers, their assistants and supervisors as well as the top managers) and general staff. Census sampling was used to select respondents in the IT department while simple random sampling was used to select individual respondents from the rest of the departments who would fill in the questionnaires.

Table 3. 1 Sampling Frame of Target Population

	Hotel 1	Hotel 2	Hotel 3	Hotel 4	Totals
IT department	10	8	7	4	29
Number of managers	20	15	18	10	63
Number of employees	226	217	230	170	843
Totals	256	240	255	184	935

Source: *hotels human resource records*, 2013

3.4.2 Sample Size Determination

The hotels total employee numbers were nine hundred and thirty five (935). According to Business Advocacy (2013), the following formulae was used to calculate the sample size at 95 percent confidence level.

Formulae

$$n = \frac{N}{1+Ne^2}$$

where n = sample size N = target population (935) e = precision level (0.05)

Solution

$$n = \frac{935}{1+935*(0.05)^2}$$

n = 280

sample size = 280 respondents

Table 3. 2: Sample Size Distribution

Hotels	Sample Size	IT department	employees
Hotel 1	76	10	66
Hotel 2	73	8	65
Hotel 3	75	7	68
Hotel 4	56	4	52
Total	280	29	250

Source: *Authors, 2013*

3.5 Data Collection

Both primary and secondary data was used to collect data.

3.5.1 Data Types and Sources

Primary data was collected through the use of questionnaires. Structured questionnaires were administered to the employees of the selected departments of the different hotels. The questionnaires had structured questions. Semi structured questionnaire were used to obtain information from the IT department. Unstructured questions enabled the researcher to probe the respondents and clarify issues or responses solicited by the structured questions.

The secondary data was obtained from the establishments hotel reports and records, relevant books, magazines, websites and the internet material, media as well as journals both published and unpublished to provide additional data for the study.

3.5.2 Data Collection Instruments

Questionnaires were used to collect data from the respondents and aimed to capture personal information of the respondents, hotels basic information about the information systems used as well as cybercrime incidences and information security measures implemented. The questions were structured and unstructured to attain more information. The questionnaires adopted the Likert scale format. Semi-structured questionnaires were used for the employees of the IT department.

3.6 Validity and Reliability

A pilot survey was conducted in Nairobi Serena Hotel to familiarize with respondents attitudes, test question sequence, and eliminate biased questions, repetitive and ambiguous questions and also to estimate response. Five questionnaires were provided to employees in different departments and one to the IT department.

Cronbach's Alpha was used to measure reliability at a level of 0.7%. Hair *et al*., (2005) says that the generally agreed upon lower limit for Cronbach's Alpha is =>0.70 but may decrease to =>0.60 in explanatory research and increase up to ≥0.80 in studies that require more stringent reliability. The reliability results for the questionnaire was 0.824.

3.7 Data Analysis and Presentation

Data was coded and analyzed using the Statistical Package for Social Sciences (SPSS) version 21. Descriptive statistics were used to describe and summarize the data to enable meaningful description of the distribution of the scores or measurements and data were presented using frequencies, means and standard deviation. Data was further subjected to inferential statistics to test for correlation. Multiple regression was

used to measure the extent independent variable influenced the dependent variable. The following expression was used;

$$Y = \alpha + \beta_1 X_1 + \beta_2 X_2 + + \beta_3 X_3 + Є$$

Where:

Y = information security

α = Y-intercept (a constant term)

$\beta_1, \beta_2 \ldots \beta_n$ = Slope parameters (partial coefficients)

X_1 = security framework policies

X_2 = cyber-threats

X_3 = management appreciation

Є = Residual (error term)

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION AND INTERPRETATION

4.0 Overview

This chapter presents the results of data analysis. First the chapter starts with screening and cleaning the data, this is followed with findings from examination of the data in terms of descriptive analysis. The chapter concludes with findings following inferential and hypothesis testing.

4.1 Data Screening

Data Screening was conducted in order to establish whether among others, data accurately reflect the responses made by the respondents, all the data were in place and accounted for, whether there was a pattern to the missing data, whether there were any unusual or extreme responses present in the data set that could distort understanding of the phenomena under study, and whether the data met the statistical assumptions that underlie multiple regression. Consequently, data was screened for missing values, outliers, and homoscedasticity.

4.1.1 Reliability statistics

The research questionnaire was subjected to reliability a reliability test using Cronbach's Alpha. Management appreciation was found to have the highest value at 0.805 while security framework policies had the least value at 0.701. These results indicate that all the indicators that were used to measure the variables were reliable as each had a value above 0.7 threshold. The independent variables were Security framework policies (X_1) with ten indicators having a value of 0.701, Cyber-threats (X_2) with eight indicators had 0.730 and management appreciation (X_3) with six

indicators had a value of 0.805. The dependent variable information security with seven indicators had 0.789. All the four variables which had 31 indicators had a total Cronbach's Alpha of 0.824. A summary is shown in table 4.1.

Table 4. 1 Reliability Statistics

Reliability statistics	**No. of items**	**Cronbach's alpha**
Security framework policies (X_1)	10	0.701
Cyber-threats (X_2)	8	0.730
Management appreciation (X_3)	6	0.805
Information security (Y)	7	0.789
Overall reliability (X_1, X_2, X_3, Y)	31	0.824

Source: *Survey Data (2013)*

4.1.1 Response Rate

The sample population consisted the employees of the all other departments except IT and the IT department employees. A total of 280 questionnaires were distributed to 251employees and 29 to the IT department. The overall response rate to the questionnaire was 94.8% (238 respondents) for the employee questionnaires and 100% (29 respondents) for the IT department. Fowler (2002) says that while there is no agreed-upon minimum response rate, the more the responses received; the more likely it is that statistically significant conclusions about the target population will be drawn therefore response rate was deemed acceptable.

4.2 Descriptive Analysis

Descriptive statistics are used to describe the basic features of data in a study as they are used to provide simple summaries about the sample. Descriptive statistics were used in this study to give a summary of the general information of the respondents.

4.2.1 Personal Information of the Respondents

Majority of the respondents were male (53.8%) and (46.2%) were female. In addition majority of the respondents were aged between 20 to 35 years (57%, n=137), followed by those aged 36-50 years (25.7%, n=61), then those above 50 years (9.7%, n=23) and lastly those below 20 years (6.8%, n=16).

With regards to the education level, the majority had attained college education (47.9%, n=114), followed by university (23.1%, n=55), then secondary level (22.3%, n=53), followed by self-taught (4.2%, n=10) and lastly primary level (2.5%, n=6).

According to marital status, majority of the respondents were married (51.9%, n=123) followed by those that were single (30%, n=72), separated were (9.7%, n=23), and the least were divorced (8.4%, n=20).

Concerning the department currently working in, the majority were from the front office (29.1%, n=69), followed by those that were from human resource department (64%, n=27), stores and procurements (15.2%, n=36), food and beverage department (12.7%, n=30), housekeeping (9.3%, n=22), security (4.2%, n=10) and the least were finance (2.1%, n=5) and kitchen (0.4%, n=1).

Majority of the respondents had worked for 11-20yrs (44.3%, n=105), followed by 1-10years (31.6%.n=75), less than one year (14.3%, n=34) and lastly more than 20 years (9.7%, n=23). According to the level of computer knowledge, basic knowledge

was (43.6%, n=103), followed by intermediate (39.8%, n=94) and lastly (16.5%, n=39) were experts. A summary of respondents personal details are shown in table 4.2.

Table 4. 2: Personal Information of the Respondents.

Variable name		***Frequency***	***N %***
Gender	Male	128	53.8
	Female	110	46.2
Age	Below 20 yrs.	16	6.8
	20 - 35 yrs.	137	57.8
	36 - 50 yrs.	61	25.7
	Above 50 yrs.	23	9.7
Education level	Self-taught	10	4.2
	Primary	6	2.5
	Secondary	53	22.3
	College	114	47.9
	University	55	23.1
Marital status	Single	71	30
	Separated	23	9.7
	Married	123	51.9
	Divorced	20	8.4
Department	F.O	69	29.1
	F&B	30	12.7
	HR	64	27
	Stores and procurement	36	15.2
	Finance	5	2.1
	Security	10	4.2
	H.K	22	9.3
	Kitchen	1	0.4
Length worked	< 1yr	34	14.3
	1 - 10 yrs.	75	31.6
	11 - 20 yrs.	105	44.3
	>20 yrs.	23	9.7
Level of computer knowledge	Basic	103	43.6
	Intermediate	94	39.8
	Expert	39	16.5

Source: *Survey Data (2013)*

4.2.2 Security Framework Policies

The respondents were asked a series questions concerning the organizations' security framework policies. A five point likert scale was used to analyze their level of agreement with the questions that were used to measure security framework policies. The summaries of the findings from the respondents are presented in table 4.3. Majority of the respondents strongly agreed and agreed that the antivirus software was effective and this was represented by total of 53.8%, 18.1% were neutral while 28.1% represented those that strongly disagreed and those who disagreed. These findings results are consistence with IT department questionnaires where majority agreed that they use antivirus and antispyware that are leading in the market.

Concerning the hotels policy to always scan all removable storage devices, majority of the respondents strongly agreed and agreed (47.5%) while those that disagreed formed 25.2%. this results reflect the statements that majority of the employees have not completed the requisite employee training and are also not familiar with the security policies set in place.

Forty four percent (44%) of the respondents strongly agreed and agree that the hotel computers were regularly scanned for malware programs while 38.6% strongly disagreed and disagreed with the statement. Hotels did not restrict the websites that could be accessed using the hotels internet and this was reflected by a majority of the respondents disagreeing with this statement while 19.7% and 7.6% agreed and strongly agreed respectively and 21.0% being neutral. The two results above could imply that there lacks proper well documented standards and firewall procedures that control internet traffic and automatic or scheduled malware scanning.

Concerning accessibility of the departments using computers if any employee, majority of the respondents (40.3%) disagreed while those that agreed presented by a total of 23.9%. Each employee has a username and password that they used to access computers and this was presented by a total tally of 44.1% of those that agreed and strongly agreed, 17.6% and 20.2% strongly disagreed and disagreed respectively while 18.1% were neutral. However 39.1% agreed and 3.4% strongly agreed which presented a majority of the respondents, when summed together, that agreed that password and usernames are unique, 12.6% strongly disagreed, 24.4% disagreed while 20.6% were neutral.

Thirty nine point nine (39.9%) agreed that the hotels internet is password protected followed by 22.7% disagreed, 15.1% strongly disagreed, 15.5% were neutral while the least was strongly agree with 6.7%. This could imply that the basic internet security are in place such as a password to connect to the Wi-Fi. However this security measures are not regularly reviewed and changed and remain operational for long periods of time.

Concerning strict company policy concerning computer misuse, 33.6% of the respondents disagreed, 22.7% agreed, 16.8% strongly disagreed followed by neutral (13.9%) and the least was 8.0% that strongly agreed. From the responses of the IT department, security screening of employees with access to sensitive information was always conducted. This could imply that organizations were particular about the people that have access to sensitive information but did not have a documented policy on screening procedures.

The means of hotel antivirus being effective (M=3.39, SD=1.115), the hotel policy is to always scan all removable storage device (M=3.18, SD=1.159) and hotels internet

is password protected (M=3.01, SD=1.227) were slightly skewed towards anchor 4 (Agree). Computer are regularly scanned for malware (M=2.95, SD=1.250), specific website being only accessible from the hotel's internet (M=2.69, SD=1.164), hotel is monitored by CCTV cameras (M=2.81,SD=1.138), departments using computers are only accessible by authorized employees (M=2.54, SD=1.124), each employee has a username and password (M=2.93, SD=1.220), password and usernames are unique to every employee (M=2.96, SD=1.130) and there are strict policies about computer misuse (M=2.76, SD=1.247) are majorly skewed toward anchor 2 (disagreed). The summaries of the above statistics are found in the table below.

Table 4.3: Security Framework Policies

	Strongly Disagree		**Disagree**		**Neutral**		**Agree**		**Strongly Agree**		**Statistics**	
	f	%	*f*	%	*f*	%	*f*	%	*f*	%	*M*	SD
Hotel antivirus software is effective	7	2.9	60	25.2	43	18.1	90	37.8	38	16.0	3.39	1.115
The hotel policy is always to scan all removable storage devices	31	13.0	29	12.2	65	27.3	93	39.1	20	8.4	3.18	1.159
Computers are regularly scanned for malware programs	41	17.2	51	21.4	41	17.2	88	37.0	17	7.1	2.95	1.250
Specific websites can only be accessed from the hotels internet	34	14.3	89	37.4	50	21.0	47	19.7	18	7.6	2.69	1.164
Hotel is monitored by CCTV cameras	29	12.2	76	32.1	58	24.5	58	24.4	16	6.8	2.81	1.138
Departments using computers are only accessible by authorised employees	41	17.2	96	40.3	44	18.5	46	19.3	11	4.6	2.54	1.124
Each employee has a username and password	42	17.6	48	20.2	43	18.1	94	39.5	11	4.6	2.93	1.220
Passwords and usernames are unique to every employee	30	12.6	58	24.4	49	20.6	93	39.1	8	3.4	2.96	1.130
Hotels internet is password protected	36	15.1	54	22.7	37	15.5	95	39.9	16	6.7	3.01	1.227
There are strict policies about computer misuse	40	16.8	80	33.6	33	13.9	66	27.7	19	8.0	2.76	1.247

Source: *Survey Data (2013)*

4.2.3 Cyber-threats

From table 4.4 majority of the respondents agreed and strongly agreed (39.7% and 31.6% respectively) that hotel computers had a lot of viruses. This is backed-up by the statistics from the IT department where the most common cyber-threats were viruses followed by Trojans, and worms. The least occurring threats were DOS attack followed by SQL database injections and hacking. However some forms of hacking occurred followed by SQL injections and the least was DOS attacks.

A majority of the respondents agreed that the Wi-Fi password was easy to guess (35.7% agreed and 12.6% strongly agreed) while 35.3% did not know, 7.6% strongly disagreed and 8.8% disagreed with the statement. When asked if the employees shared their usernames and passwords 41.2% didn't know if it happened while those that agreed were 32.4% (agreed) and 5.9% (strongly agreed) while 6.7% strongly disagreed and 13.9% disagreed with this statement.

Majority of the respondents agreed and strongly agree (42% and 12.2% respectively) that the computer do not automatically log off when idle, 30.7% didn't know and 5% and 10.1% strongly disagreed and disagreed respectively. Concerning the accessibility of the hotels website and it being always inaccessible/down 39.1% and 8.8% agreed and strongly agreed it was true while 3.4% and 35.3% strongly disagreed and disagreed respectively with the statement.

Regarding whether it was not safe for customers to make their payments online using the hotels website (39.7% agreed and 18.1% strongly agreed), 30% did not know and 7.6% and 4.6% strongly disagreed and disagreed with this statement. The consequences of the above statement is echoed through the responses about some customers complain of unusual charges to their credit cards where those that agreed

(36.6%) and strongly agreed (20.6%) formed the majority of the respondents when summed up, 27.7% didn't know while 5% and 10.1% strongly disagreed and disagreed respectively.

The statement about the employee's ability to carry out their office work in a flash disk/cd to home, majority of the respondents who agreed formed 45.4% in total while those that disagreed were 22.7%. The averages of this section leaned towards anchor 4 which is agree. The summary of the responses are presented in table 4.4.

Table 4. 4. Cyber-threats

	Strongly Disagree		**Disagree**		**Don't know**		**Agree**		**Strongly Agree**		**Statistics**	
	f	%	*f*	%	*f*	%	*f*	%	*f*	%	*M*	SD
Hotel computers have a lot of viruses	9	3.8	10	4.2	49	20.7	94	39.7	75	31.6	3.91	1.015
Wi-Fi internet password is easy to guess	18	7.6	21	8.8	84	35.3	85	35.7	30	12.6	3.37	1.058
Employees share usernames and password	16	6.7	33	13.9	98	41.2	77	32.4	14	5.9	3.17	0.971
Computers don't automatically logs off when idle	12	5.0	24	10.1	73	30.7	100	42.0	29	12.2	3.46	1.000
The hotels website is always inaccessible/down	8	3.4	84	35.3	32	13.4	93	39.1	21	8.8	3.15	1.102
It's not safe for customers to make payments via the hotels website	18	7.6	11	4.6	71	30.0	94	39.7	43	18.1	3.56	1.078
Some customers complain of unusual charges to their credit cards	12	5.0	24	10.1	66	27.7	87	36.6	49	20.6	3.58	1.079
Employees can carry their office work in a flash-disk/ cd to home	20	8.4	34	14.3	76	31.9	75	31.5	33	13.9	3.28	1.129

Source: *Survey Data (2013)*

4.2.4 Management Appreciation

Concerning the management supporting regular training on computer use and security, a majority of the respondents agreed (47.5%) and strongly agreed (26.1%), 7.6% strongly disagreed, 7.1% disagreed while 11.8% remained neutral. This reflects the IT department's responses that regular I.S training is a must to all employees. However these results are contrary with those that a majority of the respondents have not completed the requisite IT training which could imply that either most of the employees skip training sessions or only attends the first sessions and skip the rest.

Employees in the IT department are qualified which is represented by 58.4% that agreed and strongly agreed, while 8.4% and 16.4% strongly disagreed and disagreed respectively. This is reflected by the fact that most of the respondents from the IT department have attained degree and diploma level in IT. The IT department adequate resources and these is echoed by a majority of the respondents that agreed and strongly agreed (45% and 21.8% respectively) while 17.2% disagreed in total. The IT department is adequately staffed as a majority of the respondents agreed (46.6%) and strongly agreed (20.6%), strongly disagreed (3.4%) disagree (8.0%) while 21.4% were neutral. A majority of the respondents agreed (38.2%) and strongly agreed (14.3%) that the IT department is allocated its own budget, while 7.5% strongly disagreed and 14.3% disagreed with this statement. The statement is similar to responses from the IT department where a majority of the respondents agreed that managers provides adequate infrastructure for the IT department.

Top management supports and implements decisions made by the IT department where a majority of the respondents agreed (48.1%) and strongly agreed (15.6%), while 2.1% strongly disagreed and 8.0% disagreed with the statement. The support

offered by management is negated by the responses from the IT department were majority disagreed that top management supported the security policies from the IT department. The means of the responses were skewed toward Agree (anchor 4). The summaries of the above discussions are presented in table 4.5 below.

Table 4. 5: Management Appreciation

	Strongly Disagree		Disagree		Neutral		Agree		Strongly Agree		Statistics	
	f	%	*f*	%	*f*	%	*f*	%	*f*	%	*M*	SD
The hotel management supports regular training on computer use and security	18	7.6	17	7.1	28	11.8	113	47.5	62	26.1	3.77	1.140
Employees in it department are qualified	20	8.4	39	16.4	40	16.8	99	41.6	40	16.8	3.42	1.191
IT department has adequate resources	14	5.9	27	11.3	38	16.0	107	45.0	52	21.8	3.66	1.117
IT department has enough manpower	8	3.4	19	8.0	51	21.4	111	46.6	49	20.6	3.73	0.987
Top management supports and implements decisions made by IT department	5	2.1	19	8.0	62	26.2	114	48.1	37	15.6	3.67	0.907
IT department is allocated its own budget	18	7.6	34	14.3	61	25.6	91	38.2	34	14.3	3.37	1.125

Source: *Survey Data (2013)*

4.2.5 Information Security.

From Table 4.5 below, the statement concerning access to the hotels database is restricted to management personnel only majority of the respondents agreed (41.8%) and strongly agreed (18.6%) with the statement, while 11.4% disagreed and 1.7% strongly disagreed with it.

Majority of the respondents agreed (a total of 64.2%) that only managers and supervisors can make changes in the database. This could imply that the managers have different levels of administrative passwords which restricts what one can view and change in the database.

The hotels information is stored in central database in servers where it is distributed to all computer terminals. This is supported by majority of the respondents that agreed (38.7%) and strongly agreed (24.4%) that the company's data is stored in servers or centralized database. Concerning the security of accessing the database remotely, majority of the respondent agreed and strongly agreed (44.5% and 21.8% respectively) while 4.6% strongly disagreed and 7.6% disagreed with the statement. This can be collaborated by the response that database information is encrypted while being transmitted over the internet.

Majority of the respondents (65.1%) agreed that the company's database is always up to date, while 26.5% were neutral, 2.9% strongly disagree and 5.5% disagreed. Fifty six point three percent (56.3%) of the respondents agreed that the hotels database is accessible throughout the year while 10.5% disagreed and 33.2% remained neutral. The responses of the above two responses are similar to those of the IT department where majority agreed that a backup of the database is always kept and is made available when the main database is down. The integrity of the database information is collaborated by both electronic and procedural mechanisms that assure the data held is of integrity. The means of the data are higher as they lean more towards agree (4) when rounded up. A summary of the above data is presented in table 4.6.

Table 4. 6: Information Security.

	Strongly Disagree		**Disagree**		**Neutral**		**Agree**		**Strongly Agree**		**Statistics**	
	f	%	*f*	%	*f*	%	*f*	%	*f*	%	*M*	SD
Access to the hotels database is restricted to management personnel only	4	1.7	27	11.4	63	26.6	99	41.8	44	18.6	3.64	0.967
Only managers and supervisors can edit the database	10	4.2	27	11.3	48	20.2	106	44.5	47	19.7	3.64	1.053
Company data is stored in servers/ centralised database	10	4.2	14	5.9	64	26.9	92	38.7	58	24.4	3.73	1.029
Company's database is remotely accessed via a secure internet connection	11	4.6	18	7.6	51	21.4	106	44.5	52	21.8	3.71	1.036
Company's database is up to date always	7	2.9	13	5.5	63	26.5	110	46.2	45	18.9	3.73	0.931
Hotels database is accessible through-out the year	8	3.4	17	7.1	79	33.2	95	39.9	39	16.4	3.59	0.958
Some information in the database isn't sometimes corrupt	11	4.6	20	8.4	50	21.0	89	37.4	68	28.6	3.77	1.095

Source: *Survey Data (2013)*

4.3 Factor Analysis

Factor analysis is often used by a researcher when they want to understand an underlying structure or when there is a theory about an underlying structure (Tabachnick & Fidell, 2007). Factor analysis is essential in reducing data by identifying a group or clusters of variables of the same underlying variable (DeCoster, 1998). Factor analysis has three main uses which are; to understand the structure of a set of variables, its useful in construction of a questionnaire and to reduce a data set to a more manageable size while retaining as much of the original information as possible (Field, 2009). Therefore the researcher chose to use factor analysis to reduce number of items on each variables for ease of analysis, presentation and discussion of the most significant factors that affected the research.

4.3.1. Security Framework Policies

A series of questions were asked concerning the nature of security framework policies of the organizations and responses were rated on a 5 point likert scale. Table 4.7 below shows the KMO (Kaiser Meyer Olkin) and Bartletts test. The KMO measure of sampling adequacy indicates a value of 0.794 which is above the minimum required value of 0.5. These value implies that the sample size was adequate for the variables entered for analysis. Bartletts test of sphericity that was used to test the adequacy of the correlation matrix yielded a value of 624.298 with a significance level lower than 0.001, therefore the findings implied that the factor analysis was appropriate for the study and that there was a relationship among the variables.

Table 4. 7: Kaiser Meyer Olkin and Bartletts tests for security framework policies

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.794
Bartlett's Test of Sphericity	Approx. Chi-Square	624.298
	df	45
	Sig.	.000

Source: *Survey Data (2013)*

The total variance explained was computed and only those that had eigenvalues of 1 or greater were retained. The total variance accounted for by each of the factor and the cumulative percentage are displayed in table 4.8.

Table 4. 8 Total Variance Explained for Security Framework Policies

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
Monitoring systems	3.553	35.528	35.528	3.553	35.528	35.528	3.512	35.117	35.117
Authentication systems	1.493	14.928	50.456	1.493	14.928	50.456	1.534	15.339	50.456

Extraction Method: Principal Component Analysis.
a. 3 components extracted.

Source: *Survey Data (2013)*

Only two factors that had eigenvalues greater than 1 were retained for rotation and they accounted for 35.53% and 14.93% of the total variance. These two accounted for 50.456% of the total variance while the rest accounting for 49.544% of the variance. Therefore a model with the two factors may be adequate to represent the data.

The summary of the rotated component matrix is presented in table 4.9 below. The three components were rotated using varimax criterion to reduce multi-collinearity. The sub-variables were clustered using the two component factors. The two components were: 1- monitoring and authentication systems and 2-anti-malware based systems.

Table 4. 9: Rotated Component Matrix for Security Framework Policies

	Component	
	Monitoring and authentication systems	Antimalware based
Hotel antivirus software is effective		-.629
The hotel policy is always to scan all removable storage devices		-.394
Computers are regularly scanned for malware programs	.	.774
Specific websites can only be accessed from the hotels internet	.587	
Hotel is monitored by CCTV cameras	.669	
Departments using computers are only accessible by authorized employees	.599	
There are strict policies about computer misuse	.700	
Each employee has a username and password	.774	
Passwords and usernames are unique to every employee	.749	
Hotels internet is password protected	.758	

Source: *Survey Data (2013)*

4.3.2 Cyber-threats

The KMO value for cyber-threats was 0.694 which is above the minimum of 0.5 therefore implying that the sample size was adequate for these variables to be entered for analysis. The Bartlett test of sphericity yielded a value of 639.455 with a significance level smaller than 0.001. These findings implied that factor analysis was appropriate for the study and that there existed a relationship among the variables.

Table 4. 10: KMO and Bartletts test of cyber-threats

KMO and Bartlett's Test for cyber-threats

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.694
Bartlett's Test of Sphericity	Approx. Chi-Square	639.455
	df	28
	Sig.	.000

Source: *Survey Data (2013)*

All the sub-variables under cyber-threats were reduced using factor analysis and those that had eigenvalues ≥ 1 were retained. Only three components were extracted which explained 39.67%, 16.13 and 13.68% and were security structures, attack prone and systems failure respectively. The three components explained a total of 69.48% of the variance while the rest accounted for 30.52%. The summaries are presented in table 4.11.

Table 4. 11: Total Variance Explained of Cyber-threats

Total Variance Explained of cyber-threats

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
Security structures	3.173	39.668	39.668	3.173	39.668	39.668	2.514	31.428	31.428
Attack prone	1.291	16.132	55.800	1.291	16.132	55.800	1.827	22.840	54.268
Systems failure	1.095	13.681	69.482	1.095	13.681	69.482	1.217	15.213	69.482

Extraction Method: Principal Component Analysis.

a. 3 components extracted

Source: *Survey Data (2013)*

Table 4.12 below shows the results achieved after rotated component matrix was conducted on cyber-threats. Varimax rotation was used to ensure that the chances of multi-colliniearity were reduced. The items were then clustered into three factors which were 1-security structures, 2-attack prone, and 3-systems failure.

Table 4. 12: Rotated Component Matrix for Perceived Value

Rotated Component Matrix[a]

	Component		
	Security structures	Attack prone	Systems failure
Wi-Fi internet password is easy to guess	.728		
Employees share usernames and password	.864		
Computers don't automatically logs off when idle	.881		
It's not safe for customers to make payments via the hotels website	.613		
Some customers complain of unusual charges to their credit cards		.877	
Employees can carry their office work in a flash-disk/ cd to home		.895	
Hotel computers have a lot of viruses			.669
The hotels website is always inaccessible/down			.751

a. Rotation converged in 5 iterations.

Source: *Survey Data (2013)*

4.3.3 Management Appreciation

The KMO value for sampling adequacy for management appreciation was 0.818 while the correlation matrix for Bartlett test of sphericity was 472.406 with a significance level lower than 0.001. The summary of the results are presented in the table 4.13 below.

Table 4. 13: KMO and Bartlett's test for management appreciation.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.818
Bartlett's Test of Sphericity	Approx. Chi-Square	472.406
	df	15
	Sig.	.000

Source: *Survey Data (2013)*

From all the six items that were computed for perceived value as shown in table 4.5, two factors were extracted that accounted for 69.05% of the total variance explained. The first component accounted for 52.35% while the second component accounted for 16.70%. Table 4.14 shows the results for the study.

Table 4. 14: Total Variance Explained For Management Appreciation

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
Operations	3.141	52.354	52.354	3.141	52.354	52.354
Budget	1.002	16.699	69.054	1.002	16.699	69.054

Extraction Method: Principal Component Analysis.

Source: *Survey Data (2013)*

Table 4.15 below shows the results achieved after rotated component matrix was conducted on management appreciation. Varimax rotation was used to ensure that the chances of multi-colliniearity were reduced. The items were then clustered into three factors which were 1-operations and budget.

Table 4. 15 Rotated Component Matrix for Management Appreciation

Component Matrix[a]

	Component	
	Operations	Budget
Employees in it department are qualified	.701	
IT department has adequate resources	.793	
IT department has enough manpower	.804	
Top management supports and implements decisions made by IT department	.771	
IT department is allocated its own budget		.714
The hotel conducts regular training on computer use and security	.735	

a. 2 components extracted.

Source: *Survey Data (2013)*

4.3.4 Information security

The KMO measure of adequacy indicates a value of 0.840 for information security. The correlation matrix yielded a value of 631.726. The Bartlett's test of sphericity significance level was lower than 0.001 implying that the findings were significant for the study. Table 4.16 shows a summary of the results.

Table 4. 16: KMO and Bartlett's test for Information Security.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.840
Bartlett's Test of Sphericity	Approx. Chi-Square	631.726
	df	21
	Sig.	.000

Source: *Survey Data (2013)*

Table 4.17 shows the results from total variance explained for information security. The questions adopted a 5 point likert scale format that sought to capture the opinion of the respondents concerning information security. Seven factors were computed but only two components emerged. The components were 1-information database, and 2-database restrictions. The two components accounted for 48.40% and 18.774% respectively which represented a cumulative of 67.18% while the remaining factors accounted for 32.82% of the variance.

Table 4. 17: Total Variance Explained For Information Security.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
Information database	3.388	48.402	48.402	3.388	48.402	48.402	3.285	46.922	46.922
Database restrictions	1.314	18.774	67.176	1.314	18.774	67.176	1.418	20.254	67.176

Extraction Method: Principal Component Analysis.

a.2 components extracted.

Source: *Survey Data (2013)*

Table 4.18 shows the results that were obtained after rotated component matrix. Two components were extracted after varimax rotation which resulted into two clusters which are information database and database restrictions as mentioned before. The interactions converged after 3 iterations.

Table 4. 18: Rotated Component Matrix For Information Security.

Rotated Component Matrix[a] for information security

	Component	
	Information database	Database restrictions
Access to the hotels database is restricted to management personnel only		.841
Only managers and supervisors can edit the database		.807
Company data is stored in servers/ centralized database	.785	
Company's database is remotely accessed via a secure internet connection	.850	
Company's database is up to date always	.875	
Hotels database is accessible through-out the year	.872	
Some information in the database is sometimes corrupt	.634	

a. Rotation converged in 3 iterations.

Source: *Survey Data (2013)*

4.4 Inferential statistics

Inferential statistics deal with inferences about the population based on the results obtained. The study employed a multiple linear regression analysis to analyze the data obtained from sampled employees. Multiple Linear Regression (MLR) was used to test the three hypothesis that were used for the study. This is because MLR allows for the prediction of the dependent variable (Y) from several independent variables (X_s) and therefore reveals the relative magnitudes of contributions of the independents (X_s) to the variation of dependent (Y). The independent variable was broken down to three constructs that are security framework policies (X_1), cyber-threats (X_2), and management appreciation (X_3). Each construct had concepts that were used to measure it.

4.4.1 Correlation results

Pearson correlation was calculated to establish the degree of relationship between the dependent variable (information security) and the other three sub variables of the independent variable.

The correlation matrix is extremely useful for getting a rough idea of the relationship between predictors and outcome and a preliminary look for multicollinearity (Field, 2009). The values for the Pearson correlation coefficient ranges from 0 to 1 where 0 presents no relationship at all and 1 represents perfect relationship (Tabachnick & Fidell, 2007). From table 4.19, cyber-threats versus information security ($r = 0.567$, $p = 0.0001$) and management appreciation versus information security ($r = 0.419$, $p = 0.0001$) have a strong positive correlation at 0.01 level of significance. Therefore cyber-threats and management appreciation are statistically significant as the p values are less than 0.05. These means these variables move together in the same direction whether they increase or decrease. For example if cyber-threats increases, the level of the effect on information security increases as well. However, security framework policies versus information security ($r = 0.242$, $p = 0.0001$) had a weak positive but significant correlation with each other. The p value is greater than 0.05 therefore meaning that the two are independent of each other. For example, an increase in security framework policies does not necessarily cause a resultant increase in information security.

Ignoring figures from information security, cyber-threats against security framework policy represents the highest correlation ($r = 0.323$, $p = 0.0001$). As the p value is lower than 0.05, these means that the two are dependent on each other and have a positive correlation. The lowest correlation is management appreciation against

security framework policies (r = 0.093, p = 0.078). These represents a very low correlation (r value) and that the two are independent of each other which means a change in one variable does not cause a corresponding change in the other variable (p value is greater than 0.05). The summary of the results is shown in the table 4.19 below.

Table 4. 19: Correlation Matrix

Correlation matrix					
		information security	security framework policies	cyber-threats	management appreciation
Pearson Correlation	total information security	1.000	.242	.567	.419
	security framework policies	.242	1.000	.323	.093
	cyber-threats	.567	.323	1.000	.098
	management appreciation	.419	.093	.098	1.000
Sig. (1-tailed)	information security	.	.000	.000	.000
	security framework policies	.000	.	.000	.078
	cyber-threats	.000	.000	.	.068
	management appreciation	.000	.078	.068	.419

Source: *Survey Data (2013)*

4.4.2 Model summary

To determine the aspects that could predict information security, a regression model was built where information security was regressed on the three independent sub-variables. The model developed was as shown below.

$Y = \alpha + \beta_1 X_1 + \beta_2 X_2 + + \beta_3 X_3 + Є$

Where:
Y = information security

α = Y-intercept (a constant term)

$\beta_1, \beta_2 \ldots \beta_n$ = Slope parameters (partial coefficients)

X_1 = security framework policies

X_2 = cyber-threats

X_3 = management appreciation

ϵ = Residual (error term)

Table 4.20 below shows the model summary that was generated.

Table 4. 20: Regression Model Summary

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.676[a]	.457	.450	3.49271	.457	64.742	3	231	.000	2.225

a. Predictors: (Constant), Management Appreciation, Cyber-threats, Security Framework

b. Dependent Variable: Information Security

Source: *Survey Data (2013)*

According to Mugenda and Mugenda (2003), R is the multiple correlation co-efficient between all the predictors and information security. The adjusted R square for the study 0.450 which means that the three variables that were used explained 45.0% of the variation in information security. Since R^2 values above 40% are considered high, this model could therefore explain a lot of the variation in the dependent variable.

The Durbin-Watson statistic shows whether the assumption of independent errors is tenable. The value should not be less than 1 or greater than 3. In this model, it was 2.225, meaning that the errors were independent.

4.4.3 Test for multi-collinearity

For each independent variable, tolerance is the proportion of variability of that variable that is not explained by its linear relationships with the other independent variables in the model. Tolerance ranges from 0 to 1. When tolerance is close to 0 there is high multi-colinearity of that variable with other independents and the beta coefficients become unstable. In this model, tolerance values for all the independents were above 0.5, as shown in table 4.21 below, suggesting that multi-colinearity was not a problem.

Also the table on pg. 80 illustrates the values for the β coefficients for X_1 (security framework policies), X_2 (cyber-threats), X_3 (management appreciation) and the constant. Therefore the regression equation for the model can be written as follows:

$$Y = 2.865 + 0.040X_1 + .490X_2 + .372X_3$$

The regression coefficient beta values indicates the individual contribution of the variables to a model. The β value for a variable indicates the extent the value of the dependent value changes when independent variable value were to increase by 1 when other independent variable are held at constant. A positive coefficient indicates that the predicted value of the dependent variable increases when the independent variable increases and also the opposite is true.

An example using the model above model will be as follows. The β value which is a sample estimate of the population parameter for cyber-threats is 0.490. This shows

that if cyber-threats were to increase by one unit, information security would likely also increase by 49.0%, if the other independent sub variables are kept constant.

However the standardized beta values which are measured on standard deviation units are better at showing the relative importance of the predictor variables used. From the standardized values, cyber-threats (51.8%) is the most important contributor of information security followed by management appreciation (36.5%) and lastly security framework policies (.041%).

Table 4. 21.Regression Coefficients

Regression Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	2.865	2.043		1.402	.162		
	security framework	.040	.050	.041	.803	.423	.892	1.121
	cyber-threats	.490	.049	.518	10.085	.000	.891	1.122
	management appreciation	.372	.050	.365	7.472	.000	.986	1.014

a. Dependent Variable: information security

Source: *Survey Data (2013)*

4.4.4 Research hypothesis testing

The null hypothesis was subjected to T-tests in order to test for the significance of each of the β coefficients obtained. The null hypothesis was rejected if the t values gotten were higher than the corresponding t-values from the tables at the level of confidence (95%). The null hypothesis for the study were as follows:

> Ho_1. The security framework policies adopted by selected hotels in Kenya do not ensure information security.

Ho_2. Cyber threats do not affect information security of selected hotels in Kenya.

Ho_3. Executive management support on fighting cybercrimes does not influence information security in selected hotels in Kenya.

From table 4.21 above, security framework (t = .803, p = .423) which was a measure of Ho_1 was found to be insignificant at 95% confidence interval. Therefore the null hypothesis was accepted; the security framework policies adopted by selected hotels in Kenya do not ensure information security.

The other sub variables were cyber-threats (t = 10.085, p = 0.001) and management appreciation (t = 7.472, p = 0.001). These two represented Ho_2 and Ho_3 respectively. From the t values of the two sub variables, it was found out that cyber-threats and management appreciation were significant thus the two null hypotheses (Ho_2 and Ho_3) were rejected. Therefore the alternative hypotheses were adopted for the study ($H_{2:}$ Cyber threats affect information security of selected hotels in Kenya, and $H_{3:}$ Executive management support on fighting cybercrimes influence information security in selected hotels in Kenya.) This led to the null hypothesis for the two sub variables to be rejected and therefore the alternative hypothesis were found to be true.

CHAPTER FIVE

DISCUSSION, CONCLUSION AND RECCOMENDATIONS

5.0 Overview

This chapter presents the summary of the findings, conclusions, recommendations and areas for future study based on the finding of the study. The discussions of the research was based on both descriptive and inferential statistical results of chapter four with reference to past research done on similar topics. The conclusions and recommendations drawn are in respect to the results and similar past studies.

5.1 Summary of Findings

The general objective of the study was to examine the effects of cybercrime on information security of hotels in Nairobi CBD. This was based on the premise that cybercrimes had a direct effect on information security. The study had three specific objectives which were; to investigate the nature of security framework policies adopted by the selected hotels in Kenya to ensure information security; to establish the relationship of cyber-threats and their effects on information security of selected hotels in Kenya; and to determine the executive management appreciation of the business values of IT investments in fighting cybercrimes to ensure information security in selected hotels in Kenya. The variables from the objectives were subjected to factor analysis for dimension reduction to derive subcomponents. Security framework policies (X_1) had two subcomponents which were monitoring and authentication systems, and anti-malware based systems with a correlation of .242. The second independent variable cyber threats (X_2) had three sub components which were security structures, attack prone areas and system failure that had a correlation of

0.567. The last variable was management appreciation of IT investments (X_3) which did not have subcomponent but had a correlation of 0.419.

From the correlation results of the study shows that cyber-threats was the most significant determinant of information security (X_2) followed by management appreciation of IT investments (X_3). However, security framework policies had a low positive correlation to information security.

The study had three null hypothesis that were tested and the summaries are presented in the table below.

Table 5. 1. Summary of Research Hypothesis Results.

Ho1	The security framework policies adopted by selected hotels in Kenya do not ensure information security.	Accepted
Ho2.	Cyber threats do not affect information security of selected hotels in Kenya	Rejected
Ho3.	Executive management appreciation of the business value of IT investments on fighting cybercrimes does not influence information security in selected hotels in Kenya.	Rejected

Source: regression analysis, 2013.

5.2 Discussion

5.2.1 Security Framework Policies and Information Security.

The study found out that there were some aspects of security framework policies that affected information security. Concerning the use of antivirus programs, it was found out that a majority of the respondents agreed that the hotels antivirus software was effective as most organizations used top and award winning software's in the market. Kaspersky, bit-defender and MacAfee were some of the examples given. However,

most of the respondents were not conversant with the most of the hotels policies such as the policy of scanning of removable storage devices. This was seconded by information from the IT department who said that majority of the employees were not familiar with information security policies and also that most of them had not completed the required training on security. This as a results caused complacency in following of laid down policies that opens areas for attacks on hotels information resources. On further questions it was noted that most of the security framework policies especially the antiviruses and firewall programs were not customized to the organizations and had default settings which opened organizations to be easy targets.

Majority of the respondents disagreed that the frequency of scanning for malware programs was regular which led some computers to be heavily infested with malware programs. This was as a result of settings in the antimalware being left at the users' discretion to scan and delete detected items. It was found out that monitoring systems which included controlled access to specific websites, CCTV monitoring, only authorized employees having access to computers and the existence of strict policies concerning computer misuse were put in place in the hotels. These helped to prevent physical attacks to the computer systems such as destruction of hardware that may cause system interference (Lotrionte, 2002).

The hotels also had authentications systems in place which included every employee having a username and password which were unique to each and also the hotels internet access was password protected. Despite the following existing, it was found from the responses from the IT department that these systems were not reviewed and changed frequently and that some passwords, such as computer usernames and passwords, were set only once and used for long durations of time. These

compromised the effectiveness of the systems as they made it easier to guess and therefor prone to attacks.

Organizations must therefore strive to formulate Strategies prevent attacks that exploit weaknesses of the security infrastructure and develop countermeasures, including the development and promotion of technical means of protection as well as adequate and sufficient policies to fight cybercrime effectively. Gercke (2012), says that installation of protective measures can lower the risk of attacks, but successful attacks against well-protected computer systems prove that technical protection measures can never completely stop attacks.

5.2.2: Cyber-threats Against Information Security

Respondents agreed that the hotels computers had a lot of viruses. This statement was in agreement with information collected from the IT department that stated that the company's computers experienced a lot of viruses, Trojans and worms. This was attributed to the low frequency of performing a full scan on the computers, irregular antimalware updates and the use of removable media by employees who refuse to scan or disinfect detected antimalware for fear of losing their data. Scheduling automatic and regular updates, full scans and upon detection of a threat to automatically clean it or delete the threat causing agent is one of the settings the IT department may customise. Other poor practices that occurred in the hotels were: lack of regular review of the Wi-Fi internet password making it easy to guess and acquire; employees sharing among themselves their usernames and password used to access the hotel's system; and the computers not set to automatically log-off when idle for a specified duration of time which made the hotels systems to accessed by anyone making them to be vulnerable to attacks (Gercke, 2012). Gercke (2012), recommends

to well-educate computer users to make them not be easy victims for the computer offenders.

The hotels websites were found not to be safe where a majority agreed that it was not safe to make hotel payments online. This was evidenced by sometimes customers complaining of unusual charges to their credit cards especially those who paid using online means. This could indicate that most hotels had not updated and strengthened their websites security by incorporating security certificates especially the websites that required online payment and also submitting guest personal information online for example Payment Card Industry Data Security Standards (PCI DSS) (Ekaterina, 2010). A company's firewall configuration and filtering of their Internets traffic both inbound and outbound was essential to prevent opportunistic attacks from the Internet.

However, from the information gathered from the IT department noted that the hotels only had default firewalls settings that come with either the operating systems or the antimalware programs. This resulted in inadequate protection as custom configuration of the firewall can deter the most common areas of attack as they monitor and limit access to the company's network and also malicious websites that could be visited by employees. Improperly configured firewall may result in attacks against computer data/information and also attacks against computer systems. With the increasing incorporation of Internet services by hotels as a service product for their guests and employees, with benefits of 24-hour availability and worldwide accessibility (*Power*, 2000), if offenders succeed in preventing computer systems from operating smoothly can result in great financial losses for the businesses.

5.2.3 Management Appreciation of IT Investments against Information Security

Management's approval and support of regular training of all employees on computer use and security was found to influence information security especially if employees did continual attendance of every training and finished the appropriate training. However the study found out those employees sparsely attended the training sessions as they were the same (nothing new) thus found them to be monotonous. The training needed to be up-to-date on the recent and the most common attacks the hotel could experience and advice on the ways employees could contribute to the minimization and prevention of the attacks. Also the IT department employees needed to also undergo refresher training and also encouraged to undertake additional certification courses on cyber security or information security.

It was also noted that equipping the IT department with well qualified personnel, adequate resources and manpower helped a lot in ensuring information security. Competent and highly trained IT personnel enables high and continuous protection of the information and resources of the organizations. This supports Thomas, Justin, and John (2005) who says that any information group would be incapacitated or at best semi-functional if it lacked executive management support. IT personnel should be able to custom make IT solutions for the businesses as each hotel has its own unique operating environment. Having an independent budget for the IT department ensured that they provide genuine and high-end software solutions, high quality hardware and quality workmanship without shortcuts for example pirated software (Burgess, & Power, 2008). Therefore, the IT department must have a central administration and technical standards to ensure operability and continuous access to information systems all the time (Gercke, 2012).

Bragg, (2002) recommends that management should place a serious and sustained commitment to information protection and support strategies put forward by the IT department and not play a reactionary role after a major security breach. This is because managers play an important role in resource allocation and approval of resources that are needed to maintain functioning and secure system in the organization.

5.3 Conclusion

From the research findings, conclusions can be drawn based on the independent variables, security framework policies, cyber-threats and management appreciation of IT investments on the dependent variable information security.

First, security framework policies do not affect information security. This conclusion is drawn from results of inferential statistics that led to the rejection of the null hypothesis. This was as a result of a huge percentage of the respondents being unaware and some disagreeing with the security framework policies in place.

Secondly, cyber-threats affects information security. This conclusion was supported by the fact that a majority of the respondents agreed with most of the indicators of cyber-threat affects information security. Emphasis was placed on Wi-Fi passwords, employee username and password, use of removable media and automatic logging-off of computers when idle as the most significant to ensure information security. Results from regression showed that cyber-threat were the strongest determinant of information security out of the three independent variables.

Thirdly, management appreciation of IT investments affected information security. This was supported by majority of the respondents who agreed that budgeting,

qualified IT personnel, training and retraining, and adequate resource provision for IT department affected information security.

Therefore it can be concluded that there are several dimensions of cybercrimes that affect information security and they include cyber-threats and management support of IT investments. However, security framework policies affects information security to a very small extent therefore not significant.

5.4 Recommendations

Based on the result from the study, the researcher recommends:

1. Hotels should eliminate as much payment card data as possible or obscure part of the information from paper records and computer systems.
2. The hotels should conduct a mandatory regular and comprehensive training of their employees and in addition to that follow-up on the implementation of what was covered in training.
3. The hotels firewall should be further configured/customized to limit access of malicious websites that could provide avenues for attacks for example pornographic sites and sites hosting pirated software for example torrent websites.
4. The user account control settings should be implemented to control the user rights to voluntary change the system by either installing, deleting important documents (for example database files) or uninstalling programs.
5. The hotels anti-malware programs should be configured to provide added security by scheduling most tasks and activating parental control to monitor and restrict what employees can do outside their mandate.

6. The hotels industry players and stakeholders need to come together and establish industry's benchmarks on information security and also share information concerning cybercrimes.
7. Sharing of information with the police on cybercrime attacks cases need to be encouraged and proper and regular documentation of logs should be kept to facilitate investigations.
8. Strict penalties that attract financial penalties or prosecution need to be put in place to punish and discourage employees who flout rules by circumventing company policies.
9. The IT department employees need to be kept up-to-date as some of them underperform by leaving most settings as defaults. These personnel need to customize settings to the organizations needs making to make it difficult for opportunistic attacks happening.

5.5 Areas for further research

1. The effects of cybercrime on repurchase decisions.
2. A research to quantify the cost of cybercrime to hotels.
3. To conduct the same study in different area for example Mombasa and Kisumu.

REFERENCES

Abagnale, F., & Mitnick, K. (2005). *2005 FBI Computer Crime Survey.* FBI. Retrieved from www.fbi.gov/publications/ccs2005.pdf

Adam, K. L., & Richard, G. H. (2009, April 28). *Identity Theft Targets Hospitality*. Retrieved from HospitalityTechnology: http://hospitalitytechnology.edgl.com/news/Identity-Theft-Targets-Hospitality--Protect-Guests55171

Ajibuwa, F. O. (n.d.). *Data and Information Security in Modern Day Businesses.* Honolulu USA.: Atlantic international university.

American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc., Civ. 99-185 TUC ACM, 2000 U.S. Dist. Lexis 7299 (U.S. Dist April 19, 2000).

Aron, K. (2012, September 28). *Access Kenya deploys first Polycom high definition Telepresence at tribe hotel*. Retrieved from Techweez: Technology News & Reviews: http://www.techweez.com/2012/09/28/accesskenya-deploys-first-polycom-high-definition-telepresence-at-tribe-hotel/

Bacik, S. (2008). *Building an Effective Information Security Policy Architecture.* New York: CRC Press.

Barnett, R., Bhala, S., Bown, M., Claudius, J., Grunzweig, J., Havelt, R., . . . (UK), R. J. (2012). *Trustwave 2012 Global Security Report.* TrustwaveSpiderLabs.

Barbara de Lollis. (2011, october 14). *Hotels make guest data security a top priority*. Retrieved from USA today travel: http://travel.usatoday.com/hotels/post/2011/10/starwood-hilton-work-to-protect-personally-identifiable-information/553616/1?csp=obinsite

Barnett, R., Bhala, S., Bown, M., Claudius, J., Grunzweig, J., Havelt, R., . . . (UK), R. J. (2012). *Trustwave 2012 Global Security Report.* TrustwaveSpiderLabs.

Bilger, M. et al. (2007). Elevating the Discussion on Security Management - The Data Centric Paradigm. *2nd IEEE/IFIP International Workshop on Business-driven IT Management.* IBM.

Bragg, R. (2002). *CISSP Security Management and Practices.* Pearson IT Certification. Retrieved from http://www.pearsonitcertification.com/articles/article.aspx?p=30287

Burgess, C., & R., P. (2008). *Secrets Stolen, Fortunes Lost: Preventing Intellectual Property Theft And Economic Espionage In The 21st Century.* Burlington, MA: Syngress Publishing, Inc.

Business Advocacy. (2013, January 23). Retrieved from businessadvocacy.net: http://www.businessadvocacy.net/dloads/fsSampleSize.pdf

CAPEC (2010), CAPEC-117: Data Interception Attacks. Retrieved January 28, 2012, from http://capec.mitre.org/data/definitions/117.html.

Cartwright, J., Wooff, C., Aldridge, S., & Byrne, S. (2012, September 1). *Information Security Policy*. Retrieved January 1, 2013, from www.liv.ac.uk/csd/regulations/informationsecuritypolicy.pdf

D'Amico, A., 2000, What Does a Computer Security Breach Really Cost?, The Sans Institute

DSL Reports (2011). *Network Sabotage,* Retrieved January 1, 2013, from http://www.dslreports.com/forum/r26182468-Network-Sabotage-or-incompetent-managers-trying-to-

Ekaterina, B. (2010). *An Impact of Information Security Breach on Hotel Guests' Perception of Service Quality, Satisfaction, Word-Of-Mouth and Revisit Intentions for Master of Science Degree.* University of Delaware.

Furnell, S. M. (2001). The Problem of Categorizing Cybercrime and Cybercriminals. *Australian Information Warfare and Security Conference 2001*.

GOK. (2007). Kenya Vision 2030 the popular version. Government of the Republic of Kenya.

Gordon, L. A. et al., 2003, A Framework for Using Insurance for Cyber-Risk Management, Communications of the ACM, 46(3): 81-85.

Goudie, C. (2011, April 12). Cybercrime targets companies' valuable information. abc 7 news. Retrieved September 21, 2012, from https://www.abclocal.go.com/kabc/story?section=news/iteam&id=8069141

Greenberg A. (2010, February 2). Cybercrime Checks into the Hotel Industry. Forbes.com - Magazine Article. Retrieved from http://www.forbes.com/2010/02/01/cybersecurity-breaches-trustwave-te

Hair, J., Black, C., Babin, B., & Anderson, R. (2005). Multivariate Data Analysis (6th Ed.). India: Prentice Hall.

Hancock, B., 2002, Security Crisis Management-The Basics, Computers & Security, 21(5): 397-401.

Harold F. T, & Micki K. (2007). *Information Security Management Handbook* (6th Ed.). USA: Auerbach Publications.

Jatinder, N.D. G., & Sushil, K. S. (2009). *Handbook of Research on Information Security and Assurance.* Hershey New York: Information Science Reference.

Jaya, P. (2007, September 22). *The Importance of Information Security*. The star online. Retrieved January 1, 2013, from http://biz.thestar.com.my/news/story.asp?file=/2007/9/22/business/18961777&sec=business

John, R. V., (Ed.). (2009). Computer and Information Security Handbook. Canada: Elsevier Inc.

Kelly, B. J., 1999, Preserve, Protect, and Defend, Journal of Business Strategy, 20(5): 22-26

Kevin, G. C. (2011), *Cyber Intelligence: The Huge Economic Impact of Cyber Crime*, Retrieved September 21, 2012, from http://gov.aol.com/2011/09/19/cyber-intelligence-the-huge-economic-impact-of-cyber-crime/

Kitten, T. (2012, June 26). *FTC sues hotel chain for card breaches*. The ISMG network. Retrieved September 21, 2012, from http://www.bankinfosecurity.com/ftc-sues-hotel-chain-for-card-breaches-a-4900/op-1

Krutz, R. L. & Russell, D. Vi., (2003). The CISSP Prep Guide, Gold Edition, Indianapolis, IN: Wiley.

Layton, T. P. (2007). Information Security: Design, Implementation, Measurement, and Compliance. Boca Raton, FL: Auerbach publications.

Leagal Info (2009), Crime Overview Aiding and Abetting or Accessory, Retrieved September 21, 2012, from http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory. html,

Magutu, P. O., Ondimu, G. M., & Ipu, C. J. (2011). Effects of Cybercrime on State Security: Types, Impact and Mitigations with the Fiber Optic Deployment in Kenya. IBIMA Publishing, 2011, 20. Doi: DOI: 10.5171/2011.618585

Michael, K. (2010). Managing Information Security Breaches: Studies from real life. United Kingdom: IT Governance Publishing. Retrieved September 9, 2012 From.https://www.books.google.co.ke/books?isbn=1849280959

Muema, T. (2012). Economic crime in Kenya: Kenya ranks #1 globally for economic crime. PWC Kenya. Retrieved September 10, 2012, From http://www.pwc.com.edgekey.net/ke/en/press-room/economic-crime-survey-2011-pressrelease.jhtml

Mugenda, O. M., & Mugenda, A. G. (1999). *Research Methods: Quantitative and Qualitative Approaches.* Nairobi: African Centre for Technology Studies

Needleman, E. (2012, July 6). Cybercriminals sniff out vulnerable firms. The Wall Street Journal. Retrieved September 10, 2012, from http://allthingsd.com/20120705/cybercriminals-sniff-out-vulnerable-firms/

Nutt, A. (2007, January 18). The Importance of Data Security. Enzinearticles.com. Retrieved from http://www.enzinearticles.com/?The-importance-of Data-Security&id=1682729

Oracle (2003), Security Overviews. Retrieved September 10, 2012, from http://docs.oracle.com/cd/B13789_01/ network.101/ b10777/overview.htm.

Peltier, T. R. (2002). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Boca Raton, FL: Auerbach publications.

Petrocelli, T. (2005, December 9). *The Changing Face of Data Protection*. Retrieved from InformIT: http://www.informit.com/articles/article.aspx?p=422303&seqNum=3

Philip, A. (2008). Information Security: A Manager's Guide To Thwarting Data Thieves And Hackers. (W. Timothy Coombs, Ed.). United States of America: Praeger Security International.

PJ. (2009, January 7). Why is Information Security Important? MindfulSecurity.com. Retrieved December 10, 2012, from http://mindfulsecurity.com/2009/07/01/why-is-information-security-important/

Power, R., 2001, 2001 CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends, 7(1): 1-18.

PTI Contents (2009), India: A major hub for cybercrime, Retrieved September 10, 2012, From http://business.rediff.com/ slide-show/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.htm,

Saini, H., Rao, Y. S., & Panda, T.C,. (2012). Cyber-Crimes and their Impacts: A Review. International Journal of Engineering Research and Applications (IJERA), 2(2), 202–209.

Symantec Corporation. (2011, September 7). Norton study calculates cost of global cybercrime: $144billion annually. Symantec USA.

Tagert, A. C., (n.d.). Cyber Security Challenges in Developing Nations. Retrieved from http://repository.cmu.edu/dissertations/22

Petrocelli, T. (2005, December 9). The changing face of data protection: why is data protection important to the enterprise? *InformIT*. Retrieved September 20, 2012, from http://www.informit.com/articles/article.aspx?p=422303&seqNum=3

The hospitality sector is a favorite target for criminals. (2012, June 1). Express Hospitality. Retrieved September 20, 2012, from http://download1.mwti.net/download/wikifiles/marketing/India/The_hospitality_sector_is_a_favourite_target_for_cyber_criminals_Express_Hospitality.pdf

Thomas, R. P., Justin P., & John B. (2005). Information Security Fundamentals. Washington, D.C: Auerbach Publications.

Tia, D. L., (2011, March 31). Data security basics: five security issues all hotel operators need to know. Hospitality upgrade magazine.

Tittel, E., Chapple, M., & Stewart, J. M. (2003). CISSP ®□ : Certified Information Systems Security Professional Study Guide. San Francisco, London: sybex Inc.

Warren, C. Axelrod, Jennifer L. Bayuk, & Daniel Schutzer. (2009). Enterprise Information Security and Privacy. London: Artech House, Inc.

Wil, A., (2009). Unauthorised Access: Physical Penetration Testing For IT Security Teams. United Kingdom: John Wiley & Sons, Ltd.

APPENDIX I: COVER LETTER

Dear respondent,

I am a Master of Philosophy degree student in Hospitality Management, Moi University, Kenya. As part of my studies, I am carrying out a research on "***Effect of cybercrime management on Information Security of selected hotels Nairobi***". You have been chosen to participate in the named research as a respondent.

The research is being carried out using questionnaires, and interview schedules with the sole objective of identifying how different ***cybercrimes management*** affects ***information security*** in hotels. This will give hospitality policy makers and mangers the understanding needed in formulating and implementing policies to prevent and mitigate damages of information breach caused by cybercrimes.

Any information you give is purely intended for academic purposes and will be handled with utmost confidentiality. Your contribution, participation and co-operation will be highly appreciated. Thank you.

Yours Faithfully,

Muraya Moses.

APPENDIX II: EMPLOYEE QUESTIONNAIRE

SECTION A: Demographic information

Please tick where appropriate:

1. Gender Male [ ] Female [ ]

2. Age

Below 20 years [ ] 20-35 years [ ]

36-50 years [ ] Above 50 years [ ]

3. Level of education

Self-taught [ ] Primary [ ]

Secondary [ ] College [ ]

University [ ] None [ ]

3. Marital status

Single [ ] Separated [ ]

Married [ ] Divorced [ ]

4. Department currently working in?

Front office [ ] IT department [ ]

Stores and procurement [ ] Finance [ ]

Security [ ] Housekeeping [ ]

Any Other …….

5. How long have you worked in this hotel?

Less than 1 year [ ] 11-20 years [ ]

1-10 years [ ] over 20 years [ ]

6. What your level is your knowledge of computer?

Basic [ ] intermediate [ ]

Expert [ ]

SECTION B: SECURITY FRAMEWORK AND POLICIES

7. Please tick the level of agreement with the following questions.

Key: Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

		1	2	3	4	5
SF1	The antivirus software of the hotel computers are effective against malware i.e. viruses					

SF2	It is the company's policy to always scan all removable storage devices like USB Flash Disk before using them on the computers.					
SF3	Computers are regularly scanned for malware programs (for example viruses).					
SF4	One can only access specific websites from the establishment's internet connection					
SF5	The company uses CCTV to monitor departments using computers.					
SF6	Departments using computers are accessible by authorized employees only.					
SF7	Each employee has to have a user name and password to use a computer.					
SF8	Each password and user name is unique to every employee					
SF9	the company's wireless internet is password protected					
SF11	There is a strict company policy concerning computer misuse.					

SECTION C: CYBER-THREATS

8. Please indicate your level of agreement to the statements below (refer to the key below)

	SD.	D.	N.	A.	SA.
CT1.The hotel computers have a lot of viruses	[ ]	[ ]	[ ]	[ ]	[ ]
CT2. The Wi-Fi internet password can be easily guessed	[ ]	[ ]	[ ]	[ ]	[ ]
CT3. Employees share usernames and passwords	[ ]	[ ]	[ ]	[ ]	[ ]
CT4. The computer doesn't automatically logs off when idle.	[ ]	[ ]	[ ]	[ ]	[ ]
CT5. The company's website is always inaccessible/down.	[ ]	[ ]	[ ]	[ ]	[ ]
CT6. It's safe for customers to make payments on the hotels website.	[ ]	[ ]	[ ]	[ ]	[ ]

CT7. Some customers complain of unusual charges on their

credit cards. [ ] [ ] [ ] [ ] [ ]

CT8. I can copy information to my flashdisk and take it home with me. [ ] [ ] [ ] [ ] [ ]

Key: SD = Strongly disagree D= Disagree N= Neither A = Agree SA= strongly agree

SECTION D: MANAGEMENT APPRECIATION

9. Use the key below as reference as you tick your level of agreement with the following statements below.

		1	2	3	4	5
MA1	Regular training is conducted concerning computer use and security in the hotel.					
MA2	The employees working in the IT department are qualified.					
MA3	The IT department has adequate resources					
MA4	The IT department has enough personnel in their department.					
MA5	Managers supports and implements decisions made by the IT department					
MA6	The IT department has its own budget to run the department.					

Key: 1 = Strongly disagree 2 = Disagree 3 = Neither 4 = Agree 5 = Strongly agree

SECTION E: INFORMATION SECURITY

10. Please tick your level of agreement with the statements in the boxes below.

IS1. Access to the company's database is restricted to management personnel.

Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

IS2. Only managers and supervisors can make changes to the database (edit or delete entries).

Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

IS3. Information is stored on the company servers not on each individual computers.

Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

IS4a. You can access the company's database from anywhere using a secure connection.

Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

IS4b. The company's database is up to date every time

Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

IS5. Hotels database is accessible throughout the year.

Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

IS6. Some information in the database is corrupt.

Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

APPENDIX III: IT DEPARTMENT QUESTIONNAIRE

SECTION A: GENERAL INFORMATION

1. Gender Male [ ] Female [ ]

2. Age

Below 20 years [ ] 36-50 years [ ]

20-35 years [ ] Above 50 years [ ]

3. Marital status

Single [ ] Separated [ ]

Married [ ] Divorced [ ]

4. Level of education IT education

Self-taught [ ] Certificate [ ]

Diploma [ ] Degree [ ]

Any other ……..

5. Job title in the IT department ……

6. How long have you worked in this department?

Less than 1 year [ ] 15-30 years [ ]

1-l5 years [ ] Above 30 years [ ]

7. What is the nature of your employment?

Casual [ ] Permanent [ ]

Contract [ ] any other ……..

SECTION B: SECURITY FRAMEWORK AND POLICIES

8. Please tick your level of agreement with the following statements

	1	2	3	4	5
The hotel's antivirus software and anti-spyware is effective					
Employees are familiar with the hotels information security policies					
All requisite employees have completed security awareness training					
Employees with access to concentrated amounts of Restricted Data are required to have security screening.					
Computer logs are regularly monitored for any anomaly					
Firewall configuration standards and requirements are in place and documented.					

All hotels business partners meet the requisite information security requirements.					
Backups contain sufficient information able to restore the information system to a recent, operable, and accurate state.					
Local backups of critical data is done regulary.					
Security patches and updates are downloaded regularly.					

Any other

……

……

…

SECTION C: CYBER THREATS

9. Please assign a number on the order of frequency of the following

Never very often

1 2 3 4 5 6

Viruses [ ] Trojans [ ]

Worms [ ] hacking [ ]

DoS attacks [ ] SQL injections [ ]

Any other ……

……

10. a). The hotels uses several protection for its internet network.

Yes [ ] No [ ]

b). Please list them

……..

11. Please tick in the appropriate sections below

Key: Strongly disagree [1] Agree [2] Neither [3] Disagree [4] Strongly agree [5]

	1	2	3	4	5
All custom applications software are reviewed to verify their security.					

USB flash drives are prohibited to be used by employees in the hotel.					
Validation and testing of operating system and application patches are done before deployment.					
The hotel security breaches are frequent.					

SECTION D: MANAGEMENT SUPPORT.

12. Use the key below as a reference of the statements below

	1.	2.	3.	4.	5.
IT annual budget is adequate.	[ ]	[ ]	[ ]	[ ]	[ ]
Top Management support IT security policies.	[ ]	[ ]	[ ]	[ ]	[ ]
Every employee signs a non-disclosure agreement.	[ ]	[ ]	[ ]	[ ]	[ ]
Regular information security training are a must to all employees.	[ ]	[ ]	[ ]	[ ]	[ ]
Employees user accounts are deactivated immediately they either resign, fired or transferred from the hotel	[ ]	[ ]	[ ]	[ ]	[ ]
Managers provide adequate infrastructure for the IT department (i.e. networks, hardware, etc.).	[ ]	[ ]	[ ]	[ ]	[ ]
The hotel uses genuine software's in its computers.	[ ]	[ ]	[ ]	[ ]	[ ]

Key: 1 = Strongly disagree 2 = Disagree 3 = Neither 4 = Agree 5 = Strongly agree

SECTION E: INFORMATION SECURITY

13. Please tick on your level of agreement with the statements below.

A back-up of the hotel's information is always kept.

Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

Information is encrypted while being transmitted over the internet.

Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

The hotels always uses electronic mechanisms to corroborate the integrity of data in the system (e.g. RAID, digital signatures, checksums).

Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

There are procedural mechanisms in place to corroborate the integrity of data in the system (e.g. double entry, paper trails)

Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

In the event of a system compromise, there are integrity checks that are sufficient to determine whether data has been compromised as well

Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

Double authentication is used to protect the database

Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

Computer servers are protected by access controlled doors.

Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

Accurate and complete records are kept of the backups and backup media.

Strongly disagree [1], Agree [2], Neither [3], Disagree [4] Strongly agree [5]

Any other

……

……