

**Examining the Impact of Non-Technical Security Management Factors on Information
Security Management in Health Informatics**

Dissertation

Submitted to Northcentral University

**Graduate Faculty of the School of Business and Technology Management
in Partial Fulfillment of the
Requirements for the Degree of**

DOCTOR OF PHILOSOPHY

by

ABBAS H. IMAM

**Prescott Valley, Arizona
April 2013**

UMI Number: 3570265

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



UMI 3570265

Published by ProQuest LLC 2013. Copyright in the Dissertation held by the Author.

Microform Edition © ProQuest LLC.

All rights reserved. This work is protected against unauthorized copying under Title 17, United States Code.



ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

2013©

ABBAS H. IMAM

APPROVAL PAGE

Examining the Impact of Non-Technical Security Management Factors on Information
Security Management in Health Informatics

by

Abbas H. Imam

Approved by:



May 11, 2013

Chair: Mohamad S. Hammoud, Ph.D.

Date

Member: Steven Brown, D.B.A.

Certified by:



5/15/2013

School Dean: A. Lee Smith, Ph.D.

Date

Abstract

Complexity of information security has become a major issue for organizations due to incessant threats to information assets. Healthcare organizations are particularly concerned with security owing to the inherent vulnerability of sensitive information assets in health informatics. While the non-technical security management elements have been at the center of information security activities for many years, often only the technical management components (firewall, anti-virus, etc.) have been the main area of interest for many practitioners. The problem addressed in this quantitative study was the dearth of non-technical security management perspectives in the management of information security in health informatics. Two prominent bodies of research, the theory of reasoned action and general deterrence theory were integrated to formulate the study framework. This quantitative, non-experimental study examined the impact of non-technical security management factors including organizational culture, security policy and human actions on information security management. The survey instrument was hand delivered to healthcare practitioners at Korle-Bu Teaching Hospital, as well as to technocrats at the Ministry of Health in Ghana. A total of usable 177 out of two hundred surveys were returned. Survey data were analyzed using correlation and regression analyses. The results indicated a significant positive relationship between information security management and security policy ($r=.612$, $p<.001$), organizational culture ($r=.751$, $p<.001$), and human behavior actions ($r=.646$, $p<.001$). Findings from this study confirm that when non-technical factors are better appreciated and thus incorporated into organizations' overall security strategy at the onset, effective management of information security in (healthcare) organizations is ensured. Given the seriousness of the threats to

the security environment today and the lack of effective control mechanisms in place, findings from this study could offer important and potentially new perspective on information security management issues; the growing recognition of the influences of non-technical factors for developing comprehensive information security management, particularly health organizations' security. A follow-up study on non-technical security management factors' effect on information security management would reapply the present study's instrument, and compare the combined scores between this and future studies.

DEDICATION

This dissertation is dedicated to my late father, Alhaji Haruna Isaka (^{the} Imam), who taught me that the best kind of knowledge to have is that which is learned for its own sake and beneficial to mankind. It is also dedicated to my late mother, and Hajia Hawa Abdulai, who taught me that with perseverance, even the major task can be accomplished if it is done one step at a time. Thank you for being my inspiration. I miss you both.

ACKNOWLEDGEMENTS

A number of persons have helped me along the way throughout my dissertation process and I am very appreciative. In particular, my gratitude and sincere appreciations go to my dissertation committee chair, Dr. Mohamad S. Hammoud for all his guidance, encouragement, support, and patience. I don't know what would have happen without him. Again, *shukran jazeelan*. To Dr. Steven Brown, as a committee member, he has also provided constructive comments for the proposal and the dissertation. I am also indebted to Dr. Jeffrey S. Siekpe, my external reviewer and also a friend, from Tennessee State University for reviewing the dissertation proposal and validating the questionnaire.

Next to my understanding, patient, and loving wife, Eliham, who has put up with these many years of research, and to our children Shameema and Dean for involuntarily relinquishing part of their 'time with daddy' to this research. I must also thank my terrific mother- in-law, Hajia S. Chochoo Jawula, and my baby sister, Hajia A. Sadia Haruna for their continued prayers during this dissertation process. Finally, I also thank my brothers, sister, nephews, nieces, and friends for their unrelenting support for me to chalk this milestone.

Table of Contents

List of Tables	x
List of Figures	xi
Chapter 1: Introduction	1
Background	3
Problem Statement	10
Purpose.....	11
Theoretical Framework	13
Research Questions	16
Hypotheses	17
Nature of the Study	19
Significance of the Study	21
Definitions.....	22
Summary	27
Chapter 2: Literature Review	30
The Republic of Ghana-Overview	30
State of ICT in Ghana	34
Health Informatics in Ghana	38
Information Security	45
Threats to Information Security	47
Comprehensive Information Security Management	50
Non-Technical Perspective	52
Human Behavior Actions.....	53
Information Security Policy	56
Organizational Security Culture	62
Summary	65
Chapter 3: Research Method.....	68
Research Methods and Design	71
Participants.....	77
Materials/Instruments	79
Operational Definition of Variables.....	82
Data Collection, Processing, and Analysis	86
Methodological Assumptions, Limitations, and Delimitations	87
Ethical Assurances	88
Summary	89
Chapter 4: Findings.....	91
Results.....	92
Evaluation of Findings.....	132
Summary	139

Chapter 5: Implications, Recommendations, and Conclusions	141
Implications.....	144
Recommendations.....	150
Conclusions.....	154
References.....	156
Appendixes	172
Appendix A: Informed Consent.....	173
Appendix B: CITI Training Certificate.....	174
Appendix C: Permission to Adopt Construct I	175
Appendix D: Permission to Adopt Construct II.....	176
Appendix E: Permission to Adopt Construct III.....	177
Appendix F: Permission to Conduct Survey.....	178
Appendix G: Survey Questionnaire	179
Appendix H: Participants' Gender.....	185
Appendix I: Participants' Age Group	186
Appendix J: Participants' Profession	187
Appendix K: Participants' Levels of Education	188
Appendix L: Participants' Years of Experience	189
Appendix M: Inter-item correlation matrix for Security Policy	190
Appendix N: Inter-item correlation matrix for Organizational Culture.....	191
Appendix O: Inter-item correlation matrix for Human Behavior Actions	192
Appendix P: Multiple regression of ISM on the three independent variables	193

List of Tables

Table 1	<i>Ghana – Key Telecom Parameters from 2004 to 2008</i>	37
Table 2	<i>Growth of Internet Usage</i>	48
Table 3	<i>Government Websites Offering Security Policy</i>	58
Table 4	<i>General Demographic Characteristics of Respondents</i>	93
Table 5	<i>Description of Variables in This Study</i>	94
Table 6	<i>Item Responses for Information Security Management</i>	96
Table 7	<i>Inter-Item Correlation Matrix for Information Security Management</i>	97
Table 8	<i>Item-Total Reliability Statistics for Information Security Management</i>	98
Table 9	<i>The Means for the Three sub-Domains (Confidentiality, Integrity, Availability)</i>	98
Table 10	<i>Item Responses for Information Security Policy</i>	101
Table 11	<i>Item Total Statistics for Security Policy</i>	103
Table 12	<i>Descriptive Statistics for Security Policy and sub-Dimensions</i>	103
Table 13	<i>Item Responses for Organizational Culture</i>	105
Table 14	<i>Item-Total Statistics for Organizational Culture Items</i>	106
Table 15	<i>Descriptive Statistics for Organizational Culture and sub-Dimensions</i>	107
Table 16	<i>Item responses for Human Behavior Actions</i>	109
Table 17	<i>Item-Total Reliability Statistics for Human Behavior Actions</i>	110
Table 18	<i>Descriptive statistics for Human Behavior Actions and sub-Dimensions</i>	111
Table 19	<i>Correlations Between sub-Dimensions of ISM and of Security Policy</i>	116
Table 20	<i>Multivariate Effects of ISM sub-Domain on Security Policy sub-Domain Scores.</i>	117
Table 21	<i>Subjects Effects of ISM sub-Domain on Security Policy sub-Domain Scores.</i>	118
Table 22	<i>Correlations Between sub-Dimensions of ISM and Those of Security Culture</i>	120
Table 23	<i>Multivariate Effects of ISM on organizational culture sub-domain scores.</i>	121
Table 24	<i>Effects for Multivariate Multiple Regression of ISM on Security Policy sub-Domain Scores.</i>	122
Table 25	<i>Correlations Between sub-Dimensions of ISM and Human Behavior Actions.</i>	125
Table 26	<i>Multivariate Effects of ISM sub-Domain on Human Behavior Actions sub-Domain Scores.</i>	125
Table 27	<i>Effects for Multivariate Multiple Regression of ISM on Human Behavior sub-Domain Scores.</i>	127
Table 28	<i>Correlation Coefficients Between ISM and the Three Independent Variables.</i>	129
Table 29	<i>Multivariate Effects of ISM and the Three IVs sub-Domain Scores.</i>	130
Table 30	<i>Subjects Effects Tests Between ISM and the Three IVs sub-Domain Scores</i>	131

List of Figures

<i>Figure 1.</i> Map of Ghana by Ministry of Information and Media Relations (n.d.). Accessed from http://www.mino.gov.gh/	31
<i>Figure 2.</i> Structure of Ghana's Healthcare Sector	40
<i>Figure 3.</i> Management Units of Ghana's Health Sector	41
<i>Figure 4.</i> Boxplots of Information Security Management (ISM) and sub-dimensions....	99
<i>Figure 5.</i> Boxplots for Security Policy and sub-dimensions	104
<i>Figure 6.</i> Boxplots for Organizational Culture and sub-dimensions	108
<i>Figure 7.</i> Boxplots for Human Behavior Actions and sub-dimensions.....	112
<i>Figure 8.</i> Scatterplot between ISM and Security Policy, with linear regression line.....	115
<i>Figure 9.</i> Scatterplot between ISM and Organizational Culture, with linear regression line. $R = .751$ ($p < .001$), $Y = .836 + .812x$, $R^2 = .565$, Adj. $R^2 = .562$	119
<i>Figure 10.</i> Scatterplot between ISM and Human Behavior Actions, with linear regression line. $R = .646$ ($p < .001$), $Y = 1.091 + .758x$, $R^2 = .417$, Adj. $R^2 = .414$	124

Chapter 1: Introduction

Advancements related to Information and Communication Technologies (ICTs) are playing an important role in the way modern societies function. The ICTs, a general term that includes any communication application or device such as computers, televisions, radios, cellular phones, and satellite systems, are increasingly influencing the daily lives of people as well as changing the rules of doing business (OECD, 2005). The impact of ICTs on virtually all sectors of society has become a factor that determines which countries will survive economically and which countries will remain economically isolated (Al-Fakhri, Cropf, Higgs, & Kelly, 2008). For years, many developed countries (including USA, UK, Japan, and South Korea) have long been leaders in the Information and Communication Technology (ICT), and today many developing countries have joined the pact (Bridges, 2006; IICD, n. d.).

Many policy makers have alluded to the fact that ICT deployment is not only the way to achieve economic and human development (UNDESA, 2005) but an essential strategy for economic competitiveness and growth in the coming era (Zhao & Zhao, 2009). For example, U.S. President Barack Obama was reported in the U.S. News and World Report (2009) to have said that sustained expenditure on ICT induced smart ways (broadband access, electronic medical records, green energy investments, and new computers for schools and libraries) not only create new jobs but also preserve America's competitiveness in world. Former UK Prime Minister Gordon Brown has also associated UK government's efforts to use ICT as an economic catalyst (Hinsliff, 2009).

The emergence of ICTs has had broad effects on governments, businesses, and non-governmental organizations (NGOs), as ICTs have afforded these entities more

flexibility in data management and decision-making processes (Fountain, 2005; OECD, 2005). In particular, there has been an increased emergence of ICT in the healthcare industry. Many healthcare institutions as well as individual health professionals have resorted to health informatics in the management of pertinent information assets (Cruz-Correia et al., 2005).

While touting the benefits of ICTs in today's environment, a number of researchers are equally concerned about security threats to information assets of the data involved due to incessant attacks from both within organizations and external (Bakari et al., 2005; Chang & Ho, 2006). The security problem in health informatics in particular is characterized by complexity and interdependence due to the presence of human factor (Cruz-Correia et al., 2005). In healthcare, correct and in-time medical information is needed to provide high quality care. Unavailable or unreliable information can have serious consequences for patients, such as incorrect or delayed treatment (Tawileh, Hilton & McIntosh, 2007). According to Siponen et al. (2007), humans are the heart of information security for many years, yet often only the technical perspective (firewall, anti-virus, etc) of security management has been the main area of interest for many practitioners (Beznosov & Beznosova 2007). There is the need for a more inclusion of non-technical factors in the management of information security because, as Allen (2006) warned, failure to take such action could to risks organizations' information assets. Stakeholders need to recognize the importance of nontechnical components including, management support, organizational culture, organizational policy, and human behavior in changing user attitudes and behaviors towards information security (Chang & Ho, 2006; Da Veiga & Eloff, 2009; Eloff & Eloff, 2005).

The remainder of this chapter includes introduction of ICTs in e-Government, a background summary underlining the issues in ICT and health informatics. Then the problem statement and the study purpose were discussed. The theoretical framework section of the chapter contains a discussion of concepts underpinning management of information security and the study variables. The significance of the study section includes why the study is important and contains the proposed contribution that the research makes to the field of study. Finally, the definition section includes key terms being used in the study.

Background

While the use of ICTs in the public sector is not entirely new, the introduction of Internet-driven applications into government have allow agencies to exploit diverse ways of undertaking government business beyond the old ways in which they have been operating (Ciborra, 2005; Midgets, 2005). Prior to the introduction of ICTs, governments as well as organizations, were saddled with the traditional way of management which characterized by manual transactions that often resulted in information flowing only vertically and rarely between departments (Chen, Chen, Huang, & Ching, 2006; Ciborra, 2005; Midgets, 2005; Ndou, 2004). Many terms have emerged to describe the adoption of ICTs to support internal processes of government services (Ndou, 2004). Almost all transactions occurring today include some ICT network connections. For example, while people can now use ICT applications to perform tasks such as procurement of goods and services online without ever leaving their homes or offices, government officials may use ICTs to deliver better services to their citizens.

Notwithstanding the methods engaged in conducting their tasks or the kind of services being provided by stakeholders, the infusion of ICTs driven concept involve the collection and processing of huge datasets (IICD, n.d.). According to Austin and Darby (2003), because quite a lot of these data are publicly available either by law or practice, it is now increasingly possible to create a complete profile of an individual using only the public obtainable data and exclusively discernable information. Using ICT applications, government agencies now have the capability to digitally exchange massive amounts of data, documents, still and moving images, and sound (IICD, n.d.) across different levels of an organization. In addition, organizations can now access data instantaneously regardless of where they are physically stored. These infrastructural and technological innovations provide the opportunity for governments to transform from big corporations to compact and efficient organizations (Chen et al., 2006).

Researchers in econometric and also information systems (Brush, 2007; Chen et al., 2006; Chevalleray, 2005; Ciborra, 2005; Reijswoud, 2009; Zhao & Zhao, 2009) have found proof of a strong positive relationship between GDP growth and returns on ICT investments. For example, a 2002 study conducted by the Organization for Economic Co-operation and Development (OECD) revealed that ICT investments accounted for between 0.5% and 1.3% in GDP growth per capita per annum over a number of economies between 1995 and 2000. Similarly, in a World Health Organization (WHO) (2006) survey of non-OECD member states, over 80% of the respondents indicated that Health Information Systems would be very or extremely useful (Lucas, 2008). These studies illustrate that ICTs are very important developmental tools in both the private and the public sectors (Dutta, Lanvin, & Pua, 2004).

While the adoption of ICT by many governments has provided opportunities for operational efficiency and quality of services in both private and public sectors (Ciborra, 2005), concerns about the protection of the information assets involved are being raised particularly in health informatics as risks concomitant with healthcare systems have increased due to direct and indirect inter-connectivity.

Though the use of ICT in healthcare delivery systems is not a panacea for addressing all healthcare issues, ICT adoption could still be a viable option for addressing numerous healthcare delivery problems (WHO, 2006). Several countries in the developing countries such as Ghana who have adopted the health informatics (not completely though) and are converting from old-style healthcare system to a contemporary and better organized healthcare system, have the prospective to meet the mounting stresses for valued healthcare services for their citizens (Abor, Abekah-Nkrumah, & Abor, 2008). Indeed, for countries to achieve the great potential of providing quality healthcare service, the use of ICT must be a top priority.

The inadequate status of the healthcare system in many countries has been linked to inefficiencies in data and information management (Madon et al., 2007; WHO, 2006). In order to address the concerns raised, Ghana, as well as many countries resorted to health informatics (Abor et al., 2008; WHO, 2006). Ghana's healthcare delivery system is characterized by a centralized (and largely inefficient) government system operating in parallel with privately owned institutions (Abor et al., 2008). Alongside the Ministry of Health (MoH), several non-governmental organizations (NGOs) also help provide healthcare services in Ghana (MoH, n.d.). One of the most notable features of Ghana's healthcare industry in the later part of the preceding century was vigorous criticism against

traditional systems of healthcare delivery (Abor et al., 2008). While the adoption of health informatics could significantly enhance and improve all facets of Ghana's health service delivery (MOH, n.d.), the application of informatics will be constrained by many information security related challenges if left unaddressed. One of the key challenges that could derail the implementation of health informatics is the general lack of information security management and protocols of patient identifiable information in the health sector (MOH, 2009). This lack of security management could lead to data safety and privacy being violated in a number of health informatics projects and programs hence the need for the study. Thus the recent implementation of health informatics makes Ghana a good population to study in terms of security.

One of the many risks of ICT implementation and use in healthcare delivery systems is the unintended weakness of information security management (ISM) of institutions and organizations (Ebrahim & Irani, 2005). ICT related operations require cross-agency cooperation, because the functional needs for data integration that are being processed depend on critical ICT infrastructure (Nelson, Isom, & Simek, 2006). This cross-agency cooperation is particularly important in the healthcare industry, where such information assets may contain patients' vital information, which if not properly protected, could lead to profound business and legal implications for the organization (von Solms & von Solms, 2005). While there has been an increase in the deployment of broadband Internet connections in the entire sub-Saharan Africa (SSA) region, there is no evidence of corresponding information security management implementation – a major ICT problem in the region which, if not addressed could lead to most IT businesses in the region being

blacklisted by (Comerford, 2006; Nelson et al., 2006; Olowu, 2009; Ojedokun, 2005) by the watchful establishments of cyber-security in the U.S. and the United Kingdom.

There have been an increasing number of security breaches reported over the last few years. But the problem of information security breaches is not unique to a particular country or region; it has become a global issue. For example, the number of organizations that were victims of information security breaches in the years 2001-2003 rose to 91% from 75% (Pahnila, Siponen, & Mahmood, 2007). In recent years, many reports on computer crime and vulnerabilities by organizations have been published (CERT, 2008; Computer Security Institute, 2007). The increase in reports of security threats and data abuse over the years is a clear indication of the importance of information systems security that no country or business can ignore (Saint-Germain, 2005). According to Austin and Darby (2003), the threats to information assets have necessitated the need for governments to recognize potential security concerns and quickly address those concerns in order to leverage the potential of ICTs in delivering e-Government applications. Information security practitioners need a change from the way of thinking (that technical effort alone is enough security management) in order to better protect the information assets (Eloff & Eloff, 2005).

For decades, information security professionals have recognized that solving security problems requires the use of technology, process and people (Chang & Ho, 2006). However, many information security practitioners employ only the technical measure (firewall, antivirus, antimalware, etc) and process measure (such as user logins and passwords authentication) to protect information assets from being abused (Knapp, Morris, Marshall, & Byrd, 2009). Yet these measures have not been as effective as

expected because all identifiable security actions and procedures involves human element and therefore technology process alone cannot protect information assets (Dhamija, Tygar, & Hearst, 2006; Moen, Klingsheim, Simonsen, & Hole, 2007). Indeed, an organization with a comprehensive information security management in place could better able to avert data mishandling than an organization with no any sort of security management policy(Comerford (2006; Da Dhamija et al., 2006; Herath & Rao, 2009).

Many information security researchers have advocated the inclusion of the non-technical security elements, such as organizational culture, security policy, and human behavior actions in the management of information security (Chang & Ho, 2006; Da Veiga & Eloff, 2009; Dhamija et al., 2006; Herath & Rao, 2009; Pahnla et al., 2007). According to Chang and Ho (2006), an effective information security measure requires a comprehensive security management implementation. Straub (1990) suggested that organizations should deploy deterrents measures such as security guidelines and policies in order to lessen the threat of information security breaches. Many researchers agree that having a clear cut security policy could be an indicative of effective information security management for any organization dealing with healthcare information assets (Da Veiga & Eloff, 2009; Dhamija et al., 2006; Herath & Rao, 2009; Nelson et al., 2006; Pahnla et al., 2007).

Information security researchers and practitioners have applied theoretical viewpoints and approaches in their attempt to provide an understanding of the significance of non-technical facets in the control and management of information security (Da Veiga & Eloff, 2009). The General Deterrence Theory (GDT) provides an understanding on how comprehensive security procedures could discourage illegitimate behaviors. The

GDT implies a process whereby individuals desist from acting unlawfully only if they perceive the presence of severe but appropriate sanctions (Da Veiga & Eloff, 2009; Herath & Rao, 2009; Quackenbush, 2010). The theory has been applied extensively to demonstrate that thoughtless employee behavior could put an organization's information assets in a serious trouble (Pahnila et al., 2007; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005). Another theory employed by information security researchers is the Theory of Reasoned Action (TRA). Ajzen and Fishbein developed the TRA in 1975 to predict the motivational influences of behavior that are not under an individual's wishful control (Veiga & Eloff, 2009). Predicting human behavior has been among the important objectives of numerous organizational development theories, particularly if the theory may be useful in investigating unethical behaviors (Puhakainen, 2006).

Many researchers in information security domain believe that control of information begins and ends with people, and so information security management is primarily not a technological issue (Chang & Ho, 2006). Organizations could achieve only negligible protection of their information assets if management of their security is devoid of human considerations (Chang & Ho, 2007; Da Veiga & Eloff, 2009; Puhakainen, 2006). By examining the interplay of factors such as organizational culture (leadership support and normative beliefs), security policy (user awareness and behavior intention) and human behavior actions (deterrent countermeasures and compliance behavior), this study shows that achieving an effective ISM in informatics requires the utilization of both the technical and non-technical components (Smith & Eloff, 2007).

Problem Statement

Organizations are faced with incessant security threats to their information assets caused by non-technical elements such as user's inapt actions continue to be problematic particularly in health informatics (Allen, 2006; Blyth & Kovacich, 2006). A Ponemon Institute (2011) study on security breaches caused by employee sloppiness in healthcare organizations showed over 32% increase in the past year; costing the United States' healthcare industry between \$4.2 billion – \$8.1 billion annually. This issue is also problematic in Ghana which often lacks efficient judiciary system to support the functioning of information security laws, if at all they exist, as evidenced in the country's ICT framework document (ECA, 2007; Smith & Eloff, 2005). The problem addressed in this quantitative study was the dearth of non-technical security management measures in the formulation of information security management (ISM) by stakeholders in health informatics.

While recent researches have recognized that technological factors (firewall, anti-virus, etc.) are not the only key to effective management of information assets from attacks (Beznosov & Beznosova, 2007), the role of non-technical factors including organizational culture (leadership support and normative beliefs), security policy (user awareness and behavior intention), and human behavior actions (deterrent countermeasures and compliance behavior) has seen little or no attention. Failure to include non-technical factors in security management could render the entire security measure inadequate and could expose organizations to enormous security risks (Kraemer & Carayon, 2007).

This study attempts to fill the gap in academia as research in organizations adopting a comprehensive ISM is practically a novel paradigm (Colwill, 2010). By examining the interplay of organizational culture, security policy, and human behavior actions and information security, this study showed that effective ISM requires both the technical and the non-technical components (Smith & Eloff, 2007).

Findings from this study offers not only a deeper empathy into the role of non-technical elements in ISM, but useful paradigm shift to researchers whose hitherto adoption of research approaches may have been based on an understanding of security issues only from a technical standpoint. The data from this study would also be important to countries similar to Ghana who are beginning to develop their health informatics and the necessary security protocols associated with it.

Purpose

The purpose of this non-experimental quantitative study was to examine the impact of non-technical security management factors including organizational culture (leadership support and normative beliefs), security policy (user awareness and behavior intention), and human behavior actions (deterrent countermeasures and compliance behavior) on information security management in health informatics. Non-technical security management measures play an important role in organizations ISM efforts to protect systems against accidental mishaps, intentional theft and corruption of data and applications (Bishop & Frincke, 2005; Colwill, 2010). The instrument for this study was a combination from three previously used valid and tested instruments developed from the ISO/IEC 27002 Standard. The Information Security Management Construct (ISMC) (Chang & Lin, 2007), Information Security Governance Framework (ISGF) (Da Veiga &

Eloff, 2009), and the Information Security Culture Framework (ISCF) (Sipoen et al., 2010) combined to measure the impact of information security policy, organizational culture and human behavior actions, and their dimensions on information security management .

Purposeful sampling method was used for selecting the participants for this study. The population for the study included healthcare professionals from the Korle-Bu Teaching Hospital, which include physician consultants, surgeons, anesthetists, pharmacists, nurses/midwives, pathologists, radiologists, and laboratory technologists as well as technocrats from the Ministry of Health in Ghana. The optimal sample size of 56 was determined by G*Power software analysis used in previous studies (Price, Dake, Murnan, Dimming, & Akpaudo, 2005). The identified sample size exceeds the recommended 10% (Trochim, 2006) of the general population of the stakeholders. To maximize the number of completed surveys, a total of 200 surveys were distributed to the study participants at Korle-Bu Teaching Hospital, as well as the Ministry of Health in Ghana.

A Likert-type scale was used to examine the impact of non-technical security management factors on information security management in health informatics. The dependent variable for the study was Information Security Management (Survey Items 6, 7, 8, 9, 10, and 11). The independent variables were Information Security Policy (Survey Items 12, 13, 14, 15, 16, 17, 18, and 19), Organizational Culture (Survey Items 20, 21, 22, 23, 24, 25, 26, and 27), and Human Behavior Actions (Survey Items 28, 29, 30, 31, 33, 34, and 35). Data were initially formulated using standard summary statistics (means, standard deviations, frequencies, and percentages). Pearson's correlations were used to

find the relationships between ISM and its dimensions, and the salient variables (information security policy, organizational culture, human behavior actions) and their dimensions.

Theoretical Framework

The fundamental principle of this study was information security management practices of the health informatics in Ghana. As organizations gradually invest, create, and implement information communication technology (ICT) related systems, the issue of the non-technical aspects of information security management extremely important (Albrechtsen, 2007; Puhakainen, 2006). With advances in ICT, many everyday computing actions and behaviors are being computerized in order to lessen the tasks and time burdens (Pahnila et al., 2007; Siponen et al., 2010). Yet, behaviors are hard to predict (Siponen et al., 2010) and therefore information security issues cannot be addressed via technical components only. Today, many organizations deal with security management via non-technical options such as organizational culture, security policies, and human behavioral security (Chen & Lin, 2007; Puhakainen, 2006). Past studies and theories suggest relationships between non-technical factors including organizational culture, security policy and human behavioral security support, and information security (Albrechtsen, 2007; Pahnila et al., 2007). In this study therefore, two theories; the General Deterrence Theory (GDT) and the Theory of Reasoned Action (TRA) were integrated to formulate the necessary theoretical framework in examining the impact of non-technical security management elements on information security management.

General deterrence theory (GDT). The GDT, which was developed in the field of criminology, has been applied to a wide variety of domains (Quackenbush, 2010). It is

based on the presumption that people or organizations will engage in defiant activities if they do not dread some sort of rebuke (Straub and Welke, 1998; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005). Under the GDT, persons make normal choices based on their anticipated satisfaction from taking advantage of chances, against their views of the prospect and sternness of likely penalties. Though the GDT was originally used by criminologists to examine the effects of laws on crime, information systems practitioners have recently employed it to examine issues such as employees' workplace computing behaviors (Hoffer & Straub, 1989; Lee, Lee, & Yoo, 2004; Lee & Lee, 2002; Straub & Welke, 1998; Theoharidou et al., 2005; Woon & Pee, 2004).

The GDT has frequently been indirectly applied to the information systems security domain in an attempt to mitigate the threat of breaches in data security (Pahnila et al., 2007; Theoharidou et al., 2005). Parker (1983) proposed the use of deterrents such as policy and guidelines to deal with the situation of data threats. He asserted that there is the need for better empathetic of information security policy's role in detecting potential security breaches. Straub and Welke (1998) introduced the Security Action Cycle Model to postulate that information security breach must be handled at four stage levels: deter, prevent, detect, and remedy (Theoharidou et al., 2005).

There have been mixed findings about the effectiveness of deterrents measures as postulated by some researchers. While Straub (1990) and Kenkanhalli et al. (2003) have found that deterrent measures and preventive efforts both positively impact information security effectiveness, deterrent severity was found by Kenkanhalli et al. (2003) to be ineffective. In most current extended study on GDT, D'Arcy and Hovav (2007) found that severity of sanctions decreases intention to misuse information assets.

Theory of reasoned action (TRA). The TRA was developed by Fishbein and Ajzen (1975) from social psychology field in an attempt to link between beliefs, attitudes, norms, intentions, to person's actual behaviors. They proposed that, an individual's behavior intention determines one's actual behavior in the long run and that the said intention is itself being influenced by the person's attitudes, which is also in turn, determined by subjective norms towards the behavior. According to Fishbein and Ajzen (1975), subjective norm is "the person's perception that most people who are important to him think he should or should not perform the behavior in question" (Fishbein & Ajzen 1975, p. 302). Rogers & Prentice-Dunn (1997) noted that an intention based on the TRA is the most applicable measure of protection motivation.

In addition, Herath and Rao (2009) asserted that intentions could significantly influence employees' information security compliance behaviors. According to the authors, when employees perceive that their security compliance behaviors would have a favorable impact on the organization or benefit an organization, they would more likely take action. Ajzen (1991) also opined that intentions drive elements that effect on behavior, and that such intentions show the extent that individuals are prepared to try to execute the behavior in question. Ajzen further postulated that the stronger the intention to compel to involve in a behavior, the more likely the behavior will transpire. Ajzen and Fishbein (1975) proposed that the stronger the intention to comply with information security policies, the more likely the individual will actually comply with those policies.

Both the GDT and the TRA provide theoretical foundation for this study; it is hence postulated that non-technical components of security have a positive impact on the comprehensive information security management in health informatics. End-users

behaviors are hard to predict and require the application of general social psychological theories that can address relevant factors such as deterrence and normative beliefs in relationships with ISM principles. While lack of deterrents may lead to perplexity of acceptable computer usage and information assets misuse (Kleete, 1975), deterrents measures must be included in the overall information security management (Higgins et al., 2005). Individual compliance with information security management may be influenced by a wide range of formal and informal elements such as information security policy, organizational culture, and human behavior actions (Albrechtsen, 2007). As a consequence, in the context of information systems, the behavioral intentions as well as the actual behavior of managers, information systems security staff, and peers towards information systems security policy compliance will have a profound effect on the comprehensive approach to information security management.

Research Questions

As its theoretical foundation, the purpose of this non-experimental quantitative study was to examine the impact of the non-technical security management factors including organizational culture (leadership support and normative beliefs), security policy (user awareness and behavior intention), and human behavioral actions (deterrent countermeasures and compliance behavior) on information security management in health informatics. The general question this research study addresses is to what extent do non-technical security management factors influence the management of information security in the healthcare industry in Ghana.

The following questions together with null hypotheses (H_0) and alternative hypotheses (H_a) expand the above general question and serve as guide to the study:

- RQ1:** To what extent (if any) is there a relationship between security policy, as measured by user awareness and behavior intention, and Information Security Management, as measured by confidentiality, integrity, and availability?
- RQ2:** To what extent (if any) is there a relationship between organizational culture, as measured by leadership support and normative beliefs, and Information Security Management, as measured by confidentiality, integrity, and availability?
- RQ3:** To what extent (if any) is there a relationship between human behavior actions, as measured by compliance behavior and deterrent countermeasures, and Information Security Management, as measured by confidentiality, integrity, and availability?
- RQ4:** To what extent (if any) do non-technical security management factors of security policy (measured by user awareness and behavior intention), organizational culture (measured by leadership support and normative beliefs), and human behavior actions (measured by compliance behavior and deterrent countermeasures) predict Information Security Management (measured by confidentiality, integrity, and availability)?

Hypotheses

The following hypotheses were generated in order to answer and analyze the research questions of the study:

- H1₀:** **H1₀:** There is no statistically significant relationship between security policy as measured by user awareness and behavior intention, and

Information Security Management, as measured by confidentiality, integrity, and availability.

- H1_a:** There is a statistically significant relationship between security policy as measured by user awareness and behavior intention, and Information Security Management, as measured by confidentiality, integrity, and availability.
- H2₀:** There is no statistically significant relationship between organizational culture as measured by leadership support and normative beliefs, and Information Security Management, as measured by confidentiality, integrity, and availability.
- H2_a:** There is a statistically significant relationship between organizational culture as measured by leadership support and normative beliefs, and Information Security Management, as measured by confidentiality, integrity, and availability.
- H3₀:** There is no statistically significant relationship between human behavior actions as measured by compliance behavior and deterrent countermeasures, and Information Security Management, as measured by confidentiality, integrity, and availability.
- H3_a:** There is a statistically significant relationship between human behavior actions as measured by compliance behavior and deterrent countermeasures, and Information Security Management, as measured by confidentiality, integrity, and availability.

H4₀: The non-technical security management factors of security policy, organizational culture, and human behavior actions, do not significantly predict Information Security Management, as measured by confidentiality, integrity, and availability.

H4_a: The non-technical security management factors of security policy, organizational culture, and human behavior actions, are significantly predictive of Information Security Management, as measured by confidentiality, integrity, and availability.

Nature of the Study

The focus of this quantitative study was information security management of health informatics in Ghana. The study examined the impact of non-technical security management factors including information security policy, organizational culture and human behavior actions, and on information security management in Health Informatics. In choosing the research method for this study, past studies of similar objective were reviewed. Several information security researchers (Chang & Lin, 2007; Pahnla et al., 2007; Schlienger & Teufel, 2005; Straub, Boudreau, & Gefan, 2004) have used survey techniques in their studies. Therefore, similar to the research done by Chang & Lin (2007), Pahnla et al. (2009), and Schlienger and Teufel (2005), the research design of this dissertation study was focused on the use of non-experimental research techniques. Consequently, a drop-off survey methodology was chosen. Not only was the methodology relatively inexpensive, but also the results would be relatively quicker to obtain.

Nonetheless, the use of non-experimental methodology such as a survey has many disadvantages in comparison to experimental methods. According to Berry and Houston (as cited by Da Veiga & Eloff, 2009), organizations can use survey to study information security management in general, despite the fact that surveys tend to be weak in validity and reflect difficulty in determining causation (Trochim, 2006). Survey research presents all subjects with a standardized stimulus; a factor that Trochim (2006) argued may reduce the unreliability associated with a researcher's observations.

The instrument for this study was adopted from validated set of constructs used in prior studies. While the ISGF (Da Veiga & Eloff, 2009), and the ISCF (Sipoen et al., 2010) were used to measure the security policy, organizational culture and human behavior actions and their dimensions in the survey, the ISMC (Chang & Lin, 2007) was used to measure the information security management and its dimensions. Since the adopted constructs were used in different setting, a pilot test of the study instrument was needed. Thus after obtaining approval from the Institutional Review Board (IRB) of Northcentral University, a panel of two information systems university faculty members with doctoral degrees, and a medical doctor was solicited to appraise the initial instrument as part of the pilot test. The reason for the inclusion of a medical doctor in the panel in particular was to delimit bias error in the research questions.

The panel generally agreed with almost all the questions with the exception of few. Their comments were incorporated into the final version to ensure that the survey possessed satisfactory reliability and validity. Based on the panel's feedback, the number of questions was reduced from 50 to 35. Then, the survey was used to gather data from healthcare professionals from the Korle-Bu Teaching Hospital, which include physician

consultants, surgeons, anesthetists, pharmacists, nurses/midwives, pathologists, radiologists, and laboratory technologists as well as technocrats from the Ministry of Health in Ghana. I hand delivered and later picked up the research survey at the two locations. Upon completion of the data collection, the calculation of Cronbach's alpha coefficient was prepared to determine internal consistency of the instrument (Creswell, 2008).

Multiple linear regressions were used to determine the correlational relationships between information security management and salient variables from non-technical elements. Additionally, descriptive statistics was used to examine what effect, if any, the demographic information collected have on perceived information security management. Finally, internal consistency of the predictor variables was tested using Cronbach's alpha. All ethical issues such as participants' danger and agreement, the safeguarding of the data, and the interpretation of data were satisfactorily addressed.

Significance of the Study

In spite of the assertions by information systems researchers that non-technical security management issues (organizational factors, security culture, and human behavior actions) are equally important as technical issues on information security (Chang & Lin, 2007; Da Veiga & Eloff, 2009; Siponen et al., 2010), there is a dearth of academic research on comprehensive information security management (Ebrahim & Irani, 2005; Kraemer et al., 2009; Mutula, 2005). Most of these earlier researches have focused primarily on impacts of specific issues; instead of the whole issues in totality (Alfawaz, Nelson & Mohannak, 2010). Such a piecemeal approach to information security, would only solve what it is; a piece of the threats to information assets.

This study extends the knowledge base that currently exists in the field of information security beyond the perception that non-technical security management issues of information security are not as important as the technical issues (Alfawaz et al., 2010; West, 2006). Consequently, by doing this study and presenting the results to the stakeholders, information systems practitioners may be in a better position to appreciate the importance of non-technical components in having an effective information security management. Finally, this study would also contribute to the growing body of information security literature as it fills the gap in comprehensive information security management.

Definitions

The following terms pertinent to this study were defined to help the readers with the understanding of the nomenclature relative to ICT/e-Government and information security. In the Operational Definition of Variables section of chapter 3, each variable was defined in detail regarding the variable's practical usage in this research.

Anti-spyware. Yan (2005) defines spyware as software whose function includes the diffusion of personal information to a third party without the user's knowledge and unequivocal agreement. Anti-spyware is identified as the target information security application due to a number of factors.

Anti-virus. Anti-virus is described as software designed to detect, and potentially eliminate, viruses before they have had a chance to wreak havoc within the system, as well as repairing or quarantining files which have already been infected by virus activity (ISO-17799, 2005; Yan, 2005).

Availability. Availability, which is one of the six important modules of information security is a term used in the ISO-17799 (2005) to enunciate the availability

of an organization resource in an opportune way. That is, to make certain that information assets continue to be obtainable at a requisite level of performance in conditions ranging from standard through disastrous. Generally, availability of information asset is attained through redundancy involving where the information asset is stored and how it can be gotten (Dhillon & Torkzadeh, 2006).

Confidentiality. As prescribed in ISO-17799 (2005), confidentiality is guaranteeing that only authorized patrons in or outside an organization would have access to information assets. Confidentiality of an information asset could be breached in many forms. For example, allowing an individual to gaze over one's computer screen while has proprietary data displayed on it could be a breach of confidentiality. Likewise, doling out proprietary information over the telephone to somebody who is not approved to have that information may institute a breach of confidentiality (Dhillon & Torkzadeh, 2006).

Countermeasure. Countermeasure is any act, device, process, or method that decreases the susceptibility of information security structure (Rao & Herath, 2009).

Deterrence. Deterrence is defined as actions or steps such as sanctions put in place in order to dissuade someone from committing unethical or illegal acts (Straub & Welke, 1998). The aim of the deterrent measures is to discourage potential offenders from future illegal acts by instilling an understanding of the consequences.

Developed countries. Also called the industrial nations, the developed countries is a term loosely used to categorize countries whose economies are developed to what the United Nations would describe as the tertiary and quaternary (unohrlls, n.d).

Firewalls. Firewalls are security devices or software being used to curb unauthorized entree in communication networks. They prevent computer access between

communication networks, and only allow access to services which are explicitly disclosed (Beznosov & Beznosova 2007).

E-government. The term e-Government refers to is the use of any ICT based ingenuities to advance government services delivery and internal processes (Maumbe, Owei, & Alexander, 2008). Specifically, the interacting prospective offered by the ICTs has the potential to transmute the constructions and operation of governments (OECD, n.d.).

Health informatics. Health informatics refers to the “optimal use of information aided by technology to improve healthcare” (Hersh, 2009, p. 2). Health informatics has the potential to facilitate a dramatic transformation in the health care system; making the system safer, more effective and extremely efficient (Mengiste, 2010).

Information assets. Information asset is a definable part of organized Information integrated into a communication structure that is important and easily accessible to those who are required to have (Dhillon & Torkzadeh, 2006). Information assets encompass an extensive variety of corporate artifact, service and process information. Information asset could be as minute as a patient name or address file; or it may be the procedure strategies for the complete organization (Saint-Germain, 2005).

Information communication and technologies (ICTs). ICTs refer to a set of technological apparatuses and resources that provide access to information through telecommunications. It comprises of the hardware, software, networks, and media for the collection, storage, processing, transmission and presentation of information (voice, data, text, images), as well as related services (World Bank., n.d.). ICT can be split into Information Communication (IC) and Information Technology (IT). Whiles the IT refers

to the hardware and software of information collection, storage, processing, and presentation, the ICT aspect deals with the physical telecommunications systems and networks (World Bank., n.d.).

Information security management system (ISMS). The ISMS is defined as a systematic tactic to incorporating persons, procedures, and IT systems that protects grave information assets, defending them from inside and external terrorizations (Barlas, Queen, Radowitz, Shillam, & Williams, 2007).

Information security (InfoSec). Information security is defined as the conservation of confidentiality, integrity, and availability of information (Hone & Eloff, 2002). Whereas information security was initially familiarized towards technology, the term has gone past the technical aspects only into traits such as organizational, structural, and user behavior (Dhillon & Torkzadeh, 2006).

Information security culture. Information security culture is defined as suitable and often encouraged pattern of shared perceptions, attitudes and assumptions that help protect information assets of an organization (Da Veiga, & Eloff, 2007). Security culture includes both internal and external adaption of security related beliefs and security related behaviors (Schlienger & Teufel, 2005).

Information security policy. Information security policy is allows an organization and its management team to draw very clear and understandable objectives, goals, rules and formal measures that help to outline the general security stance and architecture for said organization (Hone & Eloff, 2002). It deals with the integrity, availability, and confidentiality of electronic data transmission in the information systems (Knapp et al., 2009).

Integrity. Integrity refers to the processing or services of protecting data against accidental or intentional modification, tampering and destruction (ISO/IEC 27002:2005). Data cannot be changed at random. Integrity is dishonored when a message is energetically altered in transit (Dhillon & Torkzadeh, 2006).

ISO/IEC 27002:2005. ISO/IEC 27002:2005 is an international standard that creates guiding principle and general principles for originating, applying, preserving, and refining information security management in an organization (Hone & Eloff, 2002). The purposes drawn offer general direction on the universally recognized goals of information security management (Knapp et al., 2009). The security clauses of the standard guideline are intended to be implemented to meet the requirements identified by a risk assessment.

Least developed countries (LDCs). Sometimes called third world countries, the LDCs are a group of countries that have been identified by the UN Office of the High Representative for the Least Developed Countries, Landlocked Developing Countries and Small Island Developing States as "least developed" in terms of their low gross national income (GNI), their weak human assets and their high degree of economic vulnerability (unohrlls, n.d.).

Organizational culture. Organizational culture is defined by Hofstede (2001) as the pattern of collective rudimentary norms that a group has learned as it solved the problems of external variation and internal amalgamation, which has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems.

Risk management: Risk management is the method of finding susceptibilities in the organization's information systems and taking cautiously logical steps to safeguard the confidentiality, integrity and availability of all the mechanisms in the information systems (ISO/IEC 27002:2005).

Sub-Sahara Africa (SSA). In contrast with North Africa, which is part of the Arab World (CIDA, 2008), the SSA is a geographical area of which lies south of the Sahara or those African countries which are fully or partially located south of the Sahara. The SSA, which covers an area of 24 million square kilometers, had a population of 800 million in 2007 (World Bank, 2009).

Threats to information assets. Threats to information assets are unsolicited actions that could cause thoughtful or inadvertent damage, loss or misappropriation of information assets (Dhillon & Torkzadeh, 2006; Saint-Germain, 2005).

Trojan horse. Is a spiteful, typically disparaging program concealed inside what seems to be a fascinating or valuable program, e.g., a spreadsheet, a calendar or a game. Perversely, some people cogitate a trojan horse a virus. But trojan horses, however, are not self-replicating. Instead they rely upon gullible users to spread them (SANS Institute, n.d.).

Summary

Since its advent, Information and Communication Technology (ICT) has emerged as the important tool in achieving the developmental goals of many countries (OECD, 2005). By improving access to information and by enabling communication, ICT could make government services such as education and healthcare delivery system more accessible to the general populace (IICD, n.d.). In particular, the ability to collect,

aggregate, organize, exchange, share, and re-present data economically and efficiently in the face of these challenges have already brought tremendous improvements for patients and bottom line managers (Abor et al., 2008; Bakari et al.,2005). Nevertheless, there are concerns about the threats to the informational assets involved in ICT-driven core processes. The introduction of health informatics has increased the information security threat level, considering the fact that sensitive medical records are complicated and yet flexible such that if not handled carefully they could easily be stolen, intercepted, altered, or misused (Ebrahim & Irani, 2005; von Solms, 2005).

Effective security solutions have been an elusive phenomenon (Ojedokun, 2005; von Solms, 2005; West, 2006) due the dearth of non-technical security measures in the formulation of ISM by the stakeholders in health informatics. While numerous information security surveys suggest that a large number of security incidents are due to actions or inactions of suitable (internal) users (Colwill, 2010; Puhakainen, 2006), many organizations are still generally more apprehensive with external security threats such as viruses and hacking attempts. Thus, security practitioners need to move away from the technical perspective toward the socio-organizational in order to understand human interaction and behavior in relationship to ISM (Puhakainen, 2006; von Solms, 2005). In this study the extent of influence that non-technical security management factors have on ISM in the healthcare industry in Ghana was examined.

The chapter begins with the introduction, background, the problem, and purposes of study were discussed. Next in this chapter are the theoretical basis, research questions, nature and significance of the study, and definition of terms. The rest of the dissertation is organized as follows. Chapter 2 presents sources of literature this study draws from

ICT, health informatics, and ISM. Chapter 3 describes the methodology for investigating the influence of elicited salient non-technical elements variables on ISM. While chapter 4 presents the exploratory hypotheses testing research results, chapter 5 provides a summary of the findings, review of strengths and limitations for the study, as well as managerial implications and suggestions for future research.

Chapter 2: Literature Review

The purpose of this non-experimental quantitative study was to examine the impact of the non-technical security management factors including organizational culture (leadership support and normative beliefs), security policy (user awareness and behavior intention), and human behavioral actions (deterrent countermeasures and compliance behavior) on information security management in health informatics. The objective of this chapter was to explore the relevant literature relevant to information security and health informatics constructs. The initial review covers brief overview, the state of ICT, and health informatics in Ghana. Then, literature on information security, including threats to information security, and comprehensive security management was reviewed. The final portion of the literature review contains a discussion on the importance and impact of non-technical factors relative to the management of information security. Literature was obtained for this study using electronic searches and by obtaining recently published books written about ICT, Information Security, and Health Informatics. The search sources included EBSCO Host Research Database, ProQuest Research Databases, Google Scholar, Books24x7.com, Ebrary, and NCU dissertations.

The Republic of Ghana-Overview

Formerly a British colony known as the Gold Coast, Ghana was led to independence from the British by Osagyefo Dr. Kwame Nkrumah on the 6th of March, 1957 and became the first black nation in sub-Saharan Africa to achieve independence from colonial rule. The West African country is named after the ancient empire of Ghana, from which the ancestors of the inhabitants of the present country are thought to have migrated. As shown in Figure 1, Ghana is bounded on the north by Burkina Faso, on the

east by Togo, on the south by the Atlantic Ocean, and on the west by Côte d'Ivoire. The vast majority of the country's land is tropical and partly savannah land.

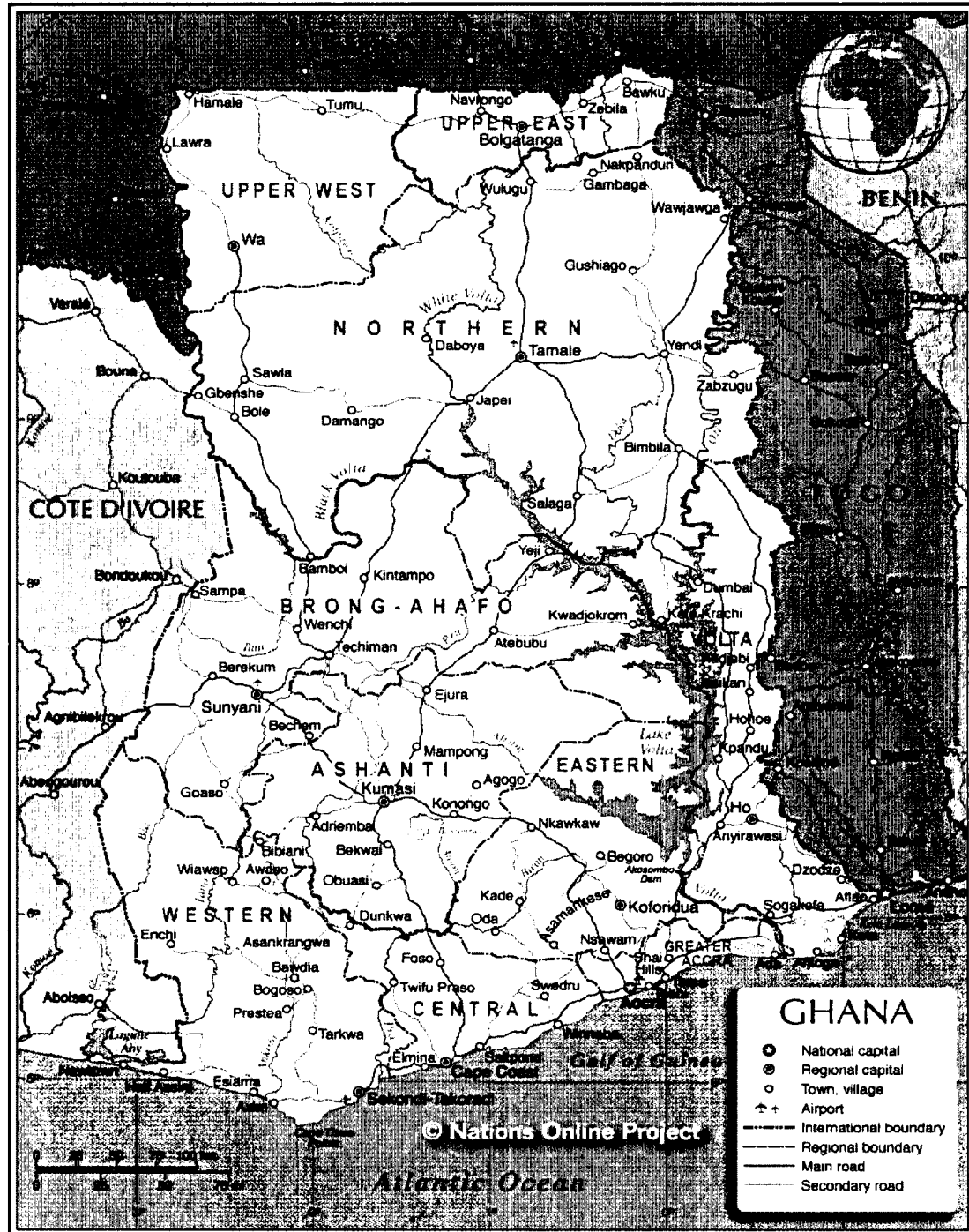


Figure 1. Map of Ghana by Ministry of Information and Media Relations (n.d.). Accessed from <http://www.mino.gov.gh/>.

A Ghana Statistical Service (GSS) on the 2010 Population and Housing Census (PHC) estimate for 2010 shows the country's population at 24.66 million, with about more than 40 percent of the population being below the age of 15. The current annual average intercensal growth rate of the population is 2.5 percent (GSS, 2012). The capital city of Accra has around 1, 673,000 people residents. Ghana's population is concentrated along the coast and in the principal cities of Accra and Kumasi. Most Ghanaians descended from migrating tribes that probably came down the Volta River valley at the beginning of the thirteenth century (MOI, n.d.). English is the official and commercial language of the country and is taught in all the schools and at all levels.

Educational system. Formal education in Ghana preceded colonization. The first schools were established by European merchants and missionaries. During the colonial period, a formal state education structure was modeled on the British system. This structure has been through a series of reforms since Ghana gained its independence in 1957. Primary and junior secondary school education is tuition-free and mandatory. The Government of Ghana's support for basic education is unequivocal. The units of the Ministry of Education, Science and Sports (MOESS) responsible for education are: the Ghana Education Service (GES), which administers pre-university education; the National Council on Tertiary Education; the National Accreditation Board; and the National Board for Professional and Technician Examinations (NABPTEX). The West African Examinations Council (WAEC), a consortium of five Anglophone West African Countries (Ghana, Nigeria, Sierra Leone, Gambia, and Liberia) is responsible for developing, administering, and grading school-leaving examinations at the secondary level. Ghana was the "shining star" of Africa at independence fifty one years ago; today it is still among the

best performing nations in Sub-Saharan Africa. The years 1960-1964 saw relatively high growth, spurred on by favorable export performance and rapid industrialization linked to import-substitution policies.

Government system. Ghana is a multiparty constitutional democracy founded on elections by open and free universal adult suffrage. The 1992 constitution that established the Fourth Republic provided a basic charter for the republican democratic government. It declares Ghana to be a unitary republic with sovereignty residing in the Ghanaian people. Intended to prevent future coups, dictatorial government, and one-party states, it is designed to establish the concept of power sharing. Executive authority is established in the Office of the Presidency, together with his Council of State. The president is head of state, head of government, and commander in chief of the armed forces. He also appoints the vice president. Legislative functions are vested in Parliament, which consists of a unicameral 230-member body plus the Speaker. To become law, legislation must have the assent of the president, who has a qualified veto over all bills except those to which a vote of urgency is attached. Members of Parliament are popularly elected by universal adult suffrage for terms of four years, except in war time, when terms may be extended for not more than 12 months at a time beyond the four years. The members are elected for a four-year term in single-seat constituencies by simple majority vote. As is predicted by Duverger's law, the voting system has encouraged Ghanaian politics into a two-party system, which means that there are two dominant political parties, with extreme difficulty for anybody to achieve electoral success under the banner of any other party. Elections have been held every four years since 1992. Presidential and parliamentary elections are held alongside each other, generally on 7 December every four years.

Economic development. On a macro-economic level, Ghana still depends on traditional natural resource export for the majority of its national income (MOC, n.d.). In those terms, it is very rich. Cocoa, its biggest export, accounts for 15% of the world's supply (GSS, n.d.). Since 1983, the economy has steadily grown. With economic recovery policies intact, the economy has raised 5% a year since 1983 (MOC, n.d.) with tourism leading the non-traditional sectors (GSS, n.d.). Furthermore, Ghana also has a good supply of gold, bauxite, diamonds, coffee, rice, cassava, timber and rubber. For example, its gold production exceeds one million fine ounces annually (GSS, n.d.). Ghana's weaknesses though, almost outweigh the strengths. Though it has remained stable and on growth course, it is said to be vulnerable due to heavy reliance on foreign borrowing. Like most countries in Africa, Ghana is in heavy debt since its independence in 1957. It also suffers from high budget deficits. With all these cash crops, costly goods, and economic restructuring, one would wonder why they need assistance at all. All of the foreign investors that come in only invest in the gold fields. Because of clearing the land for farm use and urbanization, 70% of the forest has been destroyed. With the new urban communities and mining, pollution is a very serious problem in this small nation. The Government of Ghana continues to emphasize the importance of ICT in achieving the country's objectives of diversified economic growth, increased competitiveness and transparent, accountable and efficient government (MOC, n.d.).

State of ICT in Ghana

While ICT has been recognized as the catalyst for global economic development, it took a long time for countries in the sub-Saharan Africa (SSA) to fully adopt the initiative (World Bank, 2005). The inability of countries within SSA to innovate and adopt ICTs to

their development strategies has further marginalized them, thus making the SSA countries less competitive in the global market. For example, a 1998-1999 World bank report (cited by Slater & Kwami, 2005) indicated that 50% of the sizeable economic differences between South Korea and Ghana over the past three decades can be attributed to technology development.

Ghana's economic structure is still not different from that of other countries in the SSA- the bulk of the economy is agrarian. Having recognized the value of ICTs for the socioeconomic development of any society, Ghana became one of the first countries in SAA to undertake a program of liberalization in the telecom sector (World Bank, 2009). Even though Ghana's first initiative started in late 1990s through the National Development Planning Commission (NDPC), which developed a national ICT plan, the actual process began in 1996 with the National Communications Authority (NCA) Act, which created the regulatory authority. The founding of the NCA is a demonstration of the Ghanaian government's pledge to guarantee that the country develops into an energetic partner in the global Information Society and economy (MoC, n.d.).

Ghana's practical NICI process was initiated in 2002 when the Ghanaian government established a national ICT policy and plan development committee. The framework document dubbed, *An Integrated ICT Policy and Plan Development Framework for Ghana*, was the first output of Ghana's NICI (ECA, 2007). Through the document, the government of Ghana has recognized the need for sectional plans instead of one large plan for all sectors. As a result, the ICT4D policy plan for Ghana is divided into e-commerce, education, agricultural, gender, healthcare, communication, and security sectors (MOC, n.d.). A new legislation (Legal Instrument LI 1719) was passed by

parliament in 2003, ending the exclusivity period for two telecom firms; GT and Westel. The ICT4D process is firmly apart of the political agenda and Ghana's initiative is viewed as one of the few recognized and consultative in Africa (IICD, 2008).

Irrespective of the progress made in the past years, noteworthy challenges including high cost of internet connectivity, inadequate infrastructure, lack of comprehensive information security policy, and slow uptake of e-Government applications remain in Ghana (ECA, 2007; Mutula, 2008). For example, by the end of year 2000, when the ICT policy was enacted, it was estimated that 75% of Ghana's population did not have access to basic phone service (Slater & Kwami, 2005), and average Ghanaian have no idea of how to use computers (IICD, 2008). Ghana has one of the most liberalized telecommunication sector markets in Africa. Unlike the mobile sector, the fixed-line telephone segment is almost a monopolistic market as Vodafone Ghana controls almost 98% of the market, while Airtel, the second network provider, has only 2% market share. Table 2 provides a summary of Ghana's telecommunication and ICT development from 2004 to 2008. As shown in Table 1, the number of mobile phones in Ghana exceeded the number of fixed lines by more than 40:1 with a combined telecommunication density of only just over 50% and an Internet user penetration of five percent.

Table 1
Ghana – Key Telecom Parameters from 2004 to 2008

Sector	2004	2008
Fixed-line services:		
· Total subscribers	313,000	279,000
· Annual change	4%	-26%
Internet:		
· Total users	368,000	1,100,000
· Annual change	47%	25%
· Internet penetration (population)	1.8%	4.9%
Mobile services:		
· Total subscribers (million)	1,427	11,572
· Annual change◊	83%◊	51%◊
· Mobile penetration (population)	7.0%	51%

Note. The mobile penetration jumped from 7% to 51% within four years. Adapted from “Measuring the Information Society - The ICT development index,” by International Telecommunication Union (ITU), 2009. Copyright 2009 by ITU.

Furthermore, internet charges are quite expensive and bandwidth remains a major issue (ITU, 2009). The 2009 figures released by the Ministry of Communication (MOC, n.d.) indicated that, Ghanaians pay close to 100 USD per month for the same service that their US counterparts would pay less than \$35.00. The lack of a fiber network infrastructure with national coverage in Ghana may have significant consequences for the data market than for the voice market (World Bank, 2008). Similarly, the lack of bandwidth at the Ministry of Communications to implement the government’s

pro-competitive ICT4AD and National Telecommunications Policies hamper the ICTs' ability to play a central role in driving the government's new growth agenda (MOC, n.d.).

Despite the present challenges, Ghana still abounds in massive potential for basic voice data as well as broadband data services (ITU, 2009). The country is presently in the process of enacting the first of the NICI plans that would facilitate Ghana's ICT development for the next fifteen to twenty years (ECA, 2007). It is expected that the Ghana ICT4D-2010 plan would not only deal with the sub-sector initiatives, but also would deal with the developmental initiatives and projection of the provisions of the overall ICT4D-2010 policy statement (ECA, 2007). In the 2009 budget presented to the parliament, Ghana's finance and economic planning minister reiterated that government would implement key ICT projects in 2010 to ensure that Ghana's frail manufacturing and subsistence agriculture centered economy was turned into an information and knowledge based economy (MOI, n.d.).

Health Informatics in Ghana

Generally, the Information and Communication Technology has long been recognized by international organizations (UNDP, WHO, World Bank) and national governments as one approach that supports healthcare reform initiatives of developing countries (Mengiste, 2010). In the last ten years, the call to developing countries to apply technology to their efforts at meeting the Millennium Development Goals (MDGs) has been made in several quarters. As a follow up to the year 2000 Millennium Development Declaration (MDD) by the United Nations General assembly, member states at the 58th World Health Organization (WHO) assembly adopted a resolution on e-health calling on all countries to leverage the use of informatics in the pursuit of the health-for-all vision

(Reichert, 2006; WHO, 2006). In the case of Ghana, a number of policies and strategies are available to support the country's development towards achieving sustainable health informatics (Kirigia, Seddoh, Gatwiri, Mithuri, & Seddoh, 2005).

Prior to the adoption of ICTs in to the healthcare delivery system, medical records were written on paper and then stored in locked filing cabinets, and stacked in obscure corners of hospitals buildings (Idowu, Cornford, & Bastin, 2008). Studies have shown that most medical records in developing countries cannot be used to harmonize care, regularly measure worth, or decrease medical mistakes (Hillestad et al., 2005) because health professionals usually spend long hours trying to retrieve patient data for analysis and decision-making (WHO, 2006). In addition, patients generally do not have the requisite information they needed in order to make informed decisions regarding the quality of the expected care or the cost of the expected service (Mengiste, 2010).

Healthcare system structure. Like many other countries in the SSA region, Ghana has a pluralistic healthcare system: traditional, public, private, and not-for profit mission systems ((MOH, n.d.). Until 1995, Ghana struggled to provide a comprehensive healthcare delivery system when the country began to integrate the modern health delivery system with the traditional health delivery system (Abor et al., 2008). The health system structure in Ghana is concentrated around the Ministry of Health (see Figure 1). It has a tiered organizational structure from the central headquarters in the capital city Accra to the regions, districts, and sub-districts. The primary healthcare services are carried through a grid of facilities starting with local health clinics and district health centers /hospitals, then followed by the regional hospitals providing secondary health care, and the teaching

hospitals at the zenith of providing tertiary services (MOH, n.d.). Health policy execution is carried out through the traditional public and private segments.

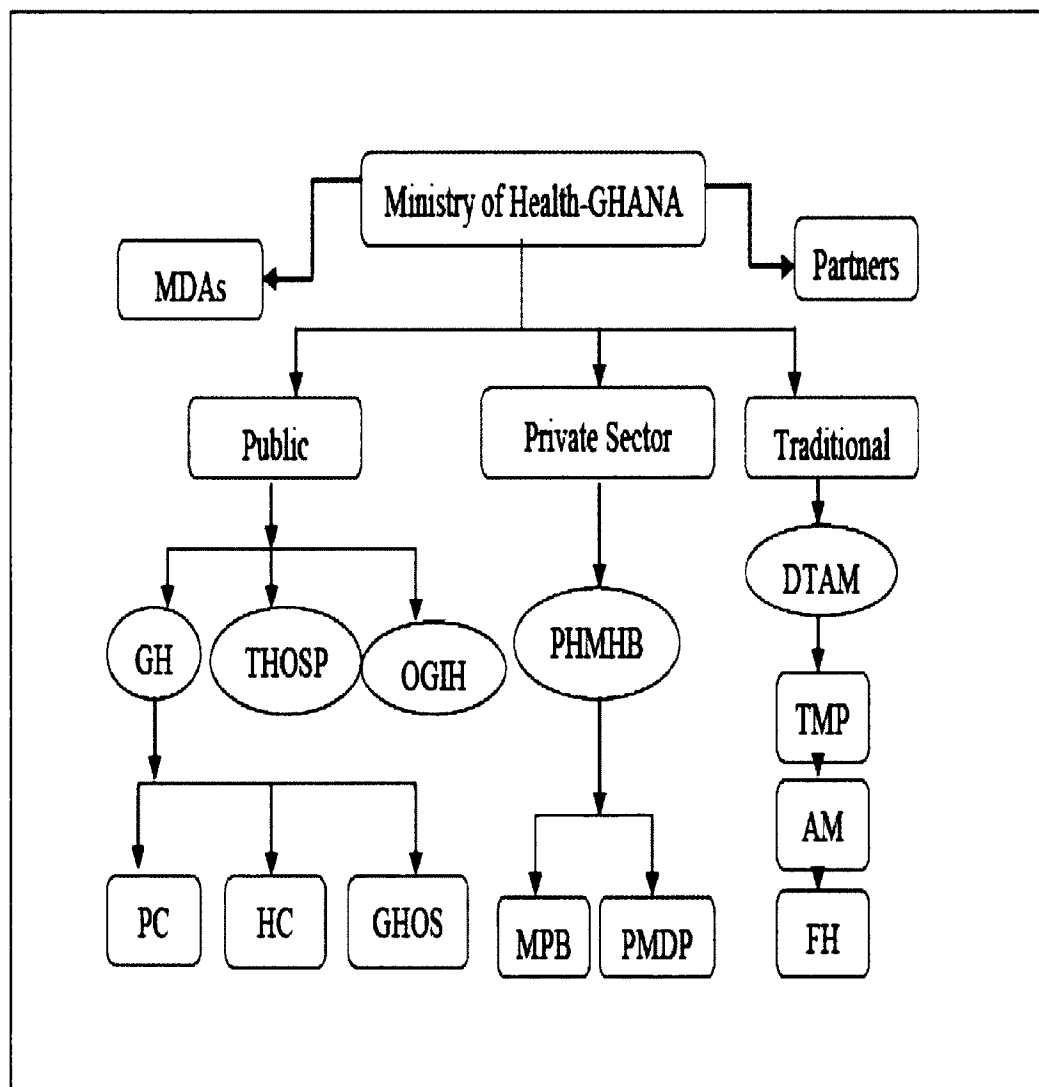


Figure 2. Structure of Ghana's Healthcare Sector

Note: MDAs-Ministries, Departments, and agencies, GHS-Ghana Health Service, THOSP-Teaching Hospitals, QGIH-Quasi Government Institution Hospital, PHMHB-Private Hospitals and Maternity Homes Board, DTAM-Department of Traditional and Alternate Medicine, GHSP-Government Hospitals, PC-Polyclinics, HC-Health Centers, MBP-Mission-Based Hospitals, PMDP-Private Medical and Dental Practitioners, AM-Alternative Medicine, FH-Faith Healers. Adopted from "An examination of hospital governance in Ghana," by Abor, P. A., Abekah-Nkrumah, G., & Abor, J. (2008). *Leadership in Health Services*, 21(1), p 3. Adopted with permission

Calls for health informatics. The health sector in Ghana is characterized by a large number of diverse management units (Figure 3) working and engendering huge quantity of information which are held in distinct silos (MOH, n.d .).

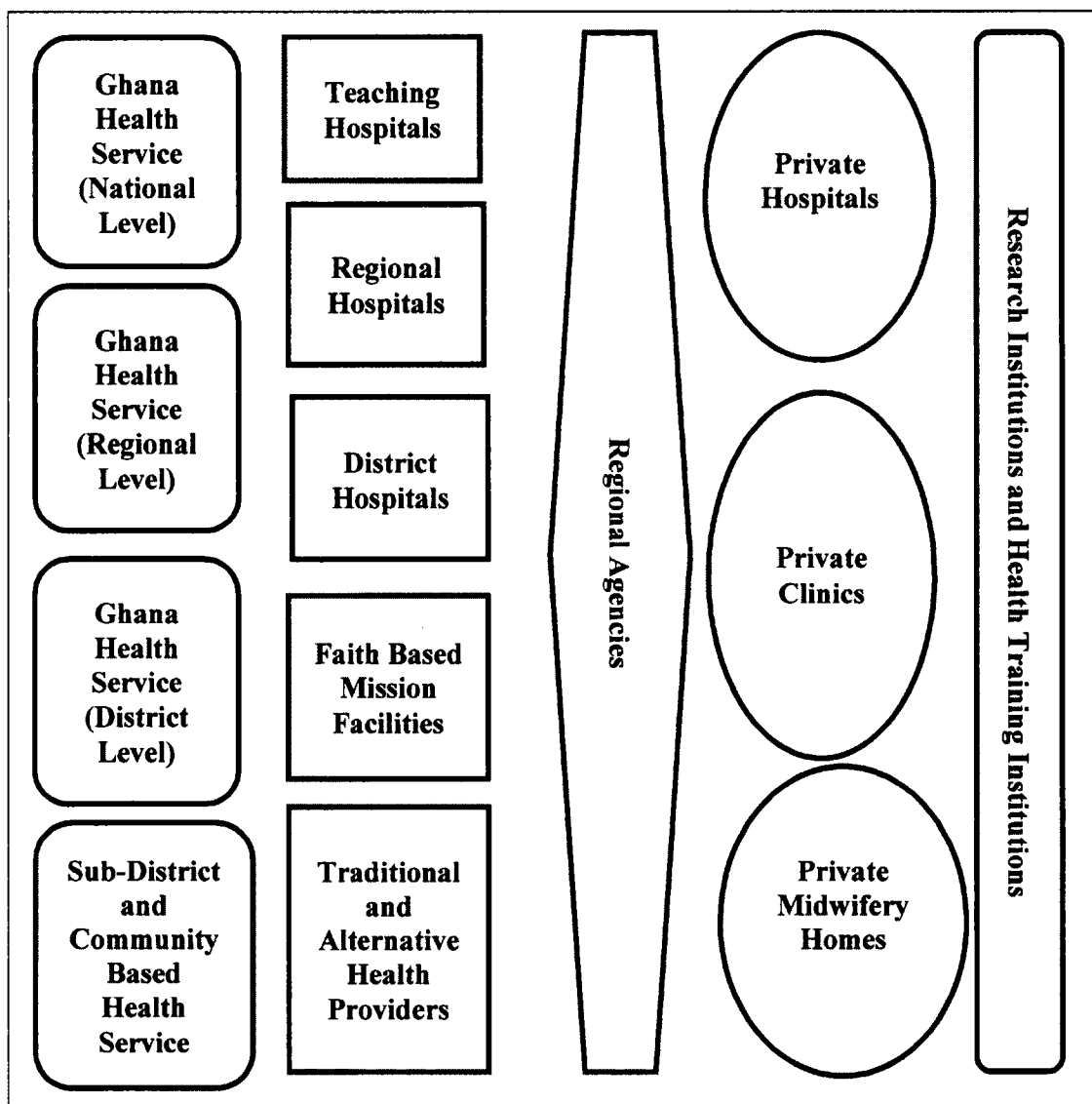


Figure 3. Management Units of Ghana's Health Sector

Note: The mobile penetration jumped from 7% to 51% within four years. Adapted from "Measuring the Information Society - The ICT development index," by International Telecommunication Union (ITU), 2009. Copyright 2012 by MOH-Ghana.

This situation generates complications in sharing information and has been an important feature in the inability of the health sector to validate its performance effectively. The numerous management components need a common platform for sharing information and the only way that can be achieved is through electronic means (MOH, n.d). As a consequence, the demand to intensify the use of ICT in the healthcare has increased. Many researchers believed that that ICT applied to health care delivery would help increase the efficiency, effectiveness, and quality of service, and also enable knowledge sharing, as well as provide the basis for networks of professionals to be supported by their fellow stakeholders.

While the overall healthcare policy and strategy for Ghana is clear and well-documented, the strategy for the relevant e-health/informatics backing to the health policy is almost non-existent (IICD, 2009). The absence of strategies for the e-health in Ghana have resulted in the implementation of initiatives that were incompatible with systems and management culture of the sector or have failed to address priorities in the health sector. The institution of ICTs in Ghana, however, has positively changed the efficiency level of the healthcare sector. With help from the International Institute for Communication and Development (IICD), Ghana's MOH has developed and published the *Health ICT Policy and Strategy* document in 2007. As outlined in the policy document, the Ghana Health Service (GHS) was established as an autonomous executive agency responsible for implementation of national policies under the control of the Minister for Health through its governing Council - the Ghana Health Service Council (GHS, n.d.). The design of the health sector ICT execution plan was intended to improve access to quality health service

by way of improving the ICT infrastructure and management of information in the health sector (MOH, n.d.).

The traditional method of health care delivery would not help Ghana achieve the Millennium Development Goals (MDGs), nor would it help the country bridge the developmental gap between them and developed countries. Thus, the introduction of informatics into the healthcare delivery system in Ghana and many other SSA countries is a strategic decision born out of the pursuit of service efficiency in the healthcare system (Zhang, Xu, Shang, & Rao, 2007). Health informatics refers to the “optimal use of information aided by technology to improve healthcare” (Hersh, 2009, p. 2). The ability of health informatics to improve the quality of health care delivery cannot be over emphasized. Mengiste (2010) suggested that health informatics has the potential to enable a dramatic transformation of the health care system, making it safer, more effective, and extremely efficient. In Ghana, the primary focus for health information technology leaders was the use of e-Health records that contain medication lists, allergies, progress notes, health maintenance information, and results for laboratory and imaging studies (MOH, n.d.). Despite evidence that health care quality, cost control, and outcomes can be improved with the use of electronic health records, adoption rates remained low (Bates, 2005; Shields et al., 2007). Through the ICTs, doctors and other healthcare professionals would have access to various medical databases which would allow them to treat patients more efficiently (Hillestad et al., 2005). The data retrieved through the use of health informatics, according to Zhang et al., (2007) would provide vital information that could have a deep effect on health care delivery system.

While health informatics is generally viewed as a catalyst for the improvement of the healthcare delivery system (Hillestad et al., 2005), there is less agreement regarding the nature and the magnitude of the impact because “at times the technology has a capacity to generate unrealistic expectations” (Lucas, 2008, p. 2123). In a 2006 survey of non-OECD countries by the WHO on potential benefits of ICT, over 80% of the respondents believed that health informatics would provide enormous benefits to the countries (Dzenowagis, 2005). Such certainty regarding the benefits of ICT, does not take the lessons of the developed countries into account (Hillestad et al., 2005). When countries in the SSA region are making strategic decisions to take advantage of health informatics related opportunities, it would be essential to take cognizance of the fact that there are many challenges in ICT connectivity across portals (Heeks, 2006; Kirigia et al., 2005). According to Fraser et al. (2005), of the many challenges that hamper the implementation and use of health informatics in the healthcare environment in the SSA, technology, cost, and security are the most common.

ICT connectivity and use varies both between and within countries (Kirigia et al., 2005). In Ghana for example, the ICT resources in the capital city Accra alone outpace the ICT resources available in the three northern regions of the country combined (MOC., n.d.). Typical health informatics set up would start from having computers and establishing local centers to transfer data, and focal Internet exchanges in the region. The data centers and exchanges require massive infrastructure such as fast connecting lines of fiber optics to link such points together to facilitate information sharing, particularly for the information in the health care delivery system (Blobel, 2007). This process of interconnectivity involves networks and portals that eventually could trigger new security

and privacy concerns that could be addressed through information security management as outlined in the ISO 27799:2008 standard (Vast, 2007); a standard that outlines rules to support the explanation and application of health informatics in ISO/IEC 27002.

Information Security

Information security is a broad and multi-dimensional topic that is described across a wide spectrum of literature. Literature reviews on the topic are vast because information security has many pretexts and no common idiolect exists inside the information security community. Some of the known expressions being used interchangeably are computer security, network security, information technology security, information systems security, and information assurance. The term “information security” will be used in the present study to describe the protection of confidentiality, integrity and availability (CIA) of information (ISO/IEC 27002, 2005). Originally orientated towards technology only, the domain of information security is broadened and encompasses aspects such as information technology, management information systems, cryptography, policy, law, finance, and economics (Dhillon & Torkzadeh, 2006).

The objective of information security is to safeguard information assets from unapproved admittance or destruction. The fundamental principles being followed in order to achieve that objective are the security triad of confidentiality, integrity, and availability (CIA). Solomon and Chapple (2005) contended that the *CIA triad* forms the basic building blocks of any good security initiative. According to Solomon and Chapple (2005), malicious individual use three primary mechanisms known as the DAD (disclosure, alteration, and denial) triad to overcome the three information security properties. Disclosure happens when the confidentiality property of information security

is breached. Confidentiality, being part of the broader privacy concept, refers to the unauthorized access, disclosure, and use of information (Dhillon & Torkzadeh, 2006). Confidentiality of information assets is guaranteeing that no one should have access to organization's proprietary information except authorized personnel or entities only. Integrity refers to the reliability and trustworthiness of the information. It is when improper modification or destruction of information takes place in transit which would lead to different result (Chang & Lin, 2007). Availability defines the timely access to data in terms of functional significance. Integrity and availability prevent any accidental or malicious alteration as well as ensures that authorized parties have access to information when needed (Dhillon & Torkzadeh, 2006).

Because many organizations rely heavily on ICTs and the data and information involved, system availability at all times becomes very important (Chang & Lin, 2007). The closer one moves toward one apex, the further one is removed from the other two. For a security breach to occur, at least one of the CIA Triad components must be compromised (Chang & Lin, 2007; Dhillon & Torkzadeh, 2006). There is an incessant discussion about extending the classic triad of confidentiality, integrity and availability despite the fact that for many years, information security professionals have held the triad to be the central principles of information security (Ezingard, McFadzean, & Birchall, 2005). For example, Parker proposed an alternative model for the classic CIA triad in 2002 which he named the six atomic elements of information (Dhillon & Torkzadeh, 2006). The model, which is known as Parkerian Hexad, comprised of the 'original' CIA triad and three other elements; possession, authenticity, and utility. We will not delve into the detail of the expanded CIA due to lack of scope and relevance to the study.

Threats to Information Security

Organizations are faced with threats to their information assets from either external or from internal regardless of their type or size (Colwill, 2010). The internal threat, which can be sub-divided into two kinds: the intentional and the unintentional can go unnoticed and is riskier than the external attack (Carroll, 2006). Intentional threat ensues when an employee or a partner in an organization shrewdly sets out to cause damage or loss of data (Kros et al., 2004). Carroll (2006) explained further that the insider threat could be anything from a dishonest employee crafting security peril for doubtful reasons or own benefit to a hacker trying to gain access to a system. Many researchers have concluded that intentional threat is more serious to information security (Carroll, 2006; Colwill, 2010; Blyth and Kovavich, 2006).

According to Colwill (2010) unintentional threat arises when an individual inside an organization inadvertently caused damage to information assets or service. According to Carroll (2006), unintentional threat could be as simple as leaving a laptop or sensitive document unattended, inadvertently install software with unidentified germ or error. Blyth and Kovavich (2006) further describe other unintentional threat actions including users' opening of email attachments without checking for viruses, downloading unauthorized software, reconfiguring of system security setting, disabling a firewall to access an unsanctioned website, and providing personal information or password to co-employees.

Disclosures of widespread security incidents have heightened information security threats. The growing insider treats, risks and impacts could be attributed to the growing usage of ICT; in particular, the Internet (Table 2).

Table 2

Growth of Internet Usage

World Regions	Population (2011 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Growth 2000-2011	Users % of Table
Africa	1,037,524,058	4,514,400	139,875,242	2,988.4 %	6.2
Asia	3,879,740,877	114,304,000	1,016,799,076	789.6 %	44.8
Europe	816,426,346	105,096,093	500,723,686	376.4 %	22.1
Middle East	216,258,843	3,284,800	77,020,995	2,244.8 %	3.4
North America	347,394,870	108,096,800	273,067,546	152.6 %	12.0
Americas / Carib.	597,283,165	18,068,919	235,819,740	1,205.1 %	10.4
Oceania / Aus.	35,426,995	7,620,480	23,927,457	214.0 %	1.1
WORLD TOTAL	6,930,055,154	360,985,492	2,267,233,742	528.1 %	100.0%

Note: While the overall percentage of Internet users in Africa is still small, the percentage increase within the last decade has been phenomenon. Table adopted with permission from "Internet usage statistics: world internet users and Population stats," a report by *Internet World Statistics*, 2009. Copyright 2001 – 2012 by Miniwatts Marketing Group.

As shown in the 2011 report by the Internet World Statistics (IWS) indicates that, Internet usage over the last decade has grown by 528.1 %. Prior to the internet becoming a phenomenon, only the military, and few government entities educational institutions had limited usage. The reason attributed to that surge in the IWS report was because internet-based businesses and transactions by both governments and businesses have become common. The increased growth in internet usage has been a concern for many information securities professional as studies have shown a direct correlation between internet usage and information security threats (Ko, Osei-Bryson, & Dorantes, 2009).

A 2009 study by the Economist Intelligence Unit (EIU) finds an increase in the number of organizations damaged by sensitive information appearing on blogs and other social media networks (Colwill, 2010). According to Ko et al. (2009), a security breach such as Denial-of-service (DoS), which occurs when cyber criminals hijack websites and in return deny everyone access, could cause an internet-dependent organization millions of dollars. Several studies on the financial impact of security breaches on statistical reports on software vulnerabilities (CERT, 2008; Kros et al., 2004), and on computer crimes (Computer Security Institute (CSI), 2007) have been published. In a 2004 study of financial institutions on global security by Deloitte and Touche (2007), more than 83% of respondents indicated that their systems had been compromised, compared to 39% in the previous year (Ko et al., 2009). Also, a 2004 CSI-FBI computer crime and security survey found that the average loss per incident from illegal access of information has increased from \$51,000 to \$300,000 and average loss from theft of information has increased to \$356,000 from \$169,000 (Gordon, Loeb, Lucyshyn, & Richardson, 2005).

According to a new Ponemon study sponsored by ID Experts, healthcare breaches continue to rise. The study report shows a whopping 90% of hospitals admit breaches cause harm to patients. As seen in Figure 3, the number of data breaches in 2011 was up 32% over 2010, averaging four data breaches per healthcare organization. To further complicate matters, 55% of healthcare organizations say they have little or no confidence they are able to detect all privacy incidents. According to the survey, 41% of healthcare data breaches of protected health information (PHI) are caused by 'sloppy employee mistakes'. Other areas causing increased risk of breaches include not knowing where patient data is located, third-party mistakes, and lost or stolen data devices (49%). These

reports on security breaches may be correlated with increased internet usage and the surge of information security threats. The problem of growing insider threats is significant, the risks are real, and the compromises and impacts are occurring. As such, there is a pressing need for more research that can highlight strategies or approaches that might reduce the threats (Doherty & Fulford, 2005).

Comprehensive Information Security Management

Information security management is defined as a methodical tactic to incorporating people, processes, and Information Technology (IT) in order to safeguard critical systems and information from both internal and external threats (Barlas, Queen, Radowitz, Shillam, & Williams, 2007). Information system practitioners, Barlas et al. (2007) suggest, must cultivate a comprehensive approach, which comprises both the human and technical dimensions when managing information security in their organizations. Facets such as organizational culture, security policies, and human behavior actions could be perceived as the non-technical aspects, while the specific technologies (firewalls, encryption, access control lists etc.) could be described as the technical traits. Information and Communication Technology (ICT) is pervasive in present-day society and pervades almost all forms of anthropological interaction. Today's ICT provides unprecedented amounts of information to organizations and their employees. As more organizations conduct their business and exchange voluminous and sensitive materials over the Internet, exposure to information security attacks is also increasing. There is the need for effective information security management (ISM) to be in place if organizations want to tackle the growing threats of computer crime to information assets from both internal and external sources.

A well planned ISM would allow information security management to know why and thus be able to develop strategic security measures to deal with the security threats. Considerable studies have been published on the varying role of information security (Da Veiga & Eloff, 2009; Eloff & Eloff, 2005; ISO/IEC) 17799: 2005; von Solms, 2006). Von Solmes (2006) discusses the development of ISM approaches over the last two decades by dividing its growth into four waves. While the growth idea was borne from technological viewpoint, it is a key timeline instrument for labeling ICT in many countries.

Information security principles are well epitomized in the relevant literature (Eloff and Eloff, 2005; Hon & Eloff, 2002; Ma, Johnston, & Pearson; Rasmussen, 2005; Ruighaver, Maynard, & Chang, 2007; Tudor, 2000). Their usefulness lies more in their character of providing guidelines for application (Knapp et al., 2009). The Generally Accepted System Security Principles (GASSP) was offered as a combined work amongst ten developed countries to cultivate a set of rules, practices and procedures (Ma et al., 2008). Eloff and Eloff (2005) also proposed the PROTECT (Policies, Risks, Objectives, Technology, Execute, Compliance and Team) method. Tudor (2000) also suggested the ISA (Information Security Architecture (ISA) approach to dealing with computer security.

The International Standards Organization/International Electro-technical Commission (ISO/IEC) 17799:2005 Code of Practice, document number 27002 (Rasmussen, 2005) is the most extensively recognized worldwide standard for ISM across industries and geography. It is also the most suitable framework for addressing information security issues in organizations and in e-Government transactions (Ma et al., 2008), as well as set of guideline for implementing comprehensive ISM framework. The

objectives and controls in ISO/IEC 17799:2005 are intended to be applied to meet the necessities recognized in risk assessment management (Knapp et al., 2009; Ma et al., 2008). The document was intended as a common foundation and real useful guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities (ISO/IEC 17799:2005).

Non-Technical Perspective

In the past, concerns about information security in most organizations tended to be focused on technical threats like viruses and intrusions (Schlienger & Teufel, 2005). Yet recent reports suggested that a large fraction of information security breaches originate from non-technical security perspective in many organizations (Gordon et al., 2005). According to Mellwrath (2006), organizations lose between 2% to 3% of their annual profits owing to internal information security incidents. Stanton et al. (2005) also cited a 2002 study by Ernst and Young which suggested that about 75% of security breaches reported were actions of employees. A number of comparable studies conclude that internal threats to information security are more serious than previously thought (Furnell, 2006). Whether these internal security breaches are intentional or not, the researchers emphasized that employees' behavior should be viewed in an information assets protection mode (Albrechtsen, 2007; COBIT, 2004; Stranton et al., 2005). In the broader sense in contemporary ICT environment, information security involves people, processes as well as technologies.

In spite of the importance of non-technical factors in safeguarding organizations' information assets (Dhillon & Torkzadeh, 2006), only few publications in the information security literature address the some level of importance of the non-technical components

(Da Veiga & Eloff, 2007; May & Lane, 2006, Ruighaver et al., 2007; Siponen & Oinas-Kukkonen, 2007). Recent management of information security recognizes the imperious of including people and processes to ensure the quality of information in contemporary organizations. Non-technical factors (organizational culture, security policy and human behavior actions) represent key components that must be addressed by stakeholders for an effective information security management (Colwill, 2010).

In this study, two theoretical frameworks-the General Deterrence Theory (GDT) and the Theory of Reasoned Action (TRA) were employed to postulate that human and organizational factors have huge impact on the management of information security and one's behavior or deed is dogged by his or her intention to perform such deed. In today's dynamic changing environments, gaining a better understanding of user behavior characteristics could help evaluate, develop and review end user behavior. Therefore, the success of information security management depends on the users' security related behavior. Details of the theories have already been provided in the theoretical framework section in chapter 1.

Human Behavior Actions

The role of human and organizational factors has been examined from a range of disciplinary perspective (Karemer, Carayon, & Clem, 2009). Human behavior in ICT is now considered one of the key slits in the array of information security management (Caroll, 2006). According to Herath and Rao (2009), organizations often rely on security policies in situations when security technologies could not addressed human behaviors issues such as proper use of computer and network resources, appropriate password habits. Literature has revealed that many recent information security studies are not only on areas

such as awareness, insider computer crime, governance, and policy compliance (Kruger & Kearney, 2006; Vroom & von Solms, 2004) but are also focused on the human component aimed at the threat that human behavior might pose to the protection of information assets. Human beings have both strengths and weaknesses in relation to information security tasks. Carroll (2006) described end users as both threats and as well as resources for information security management in organizations.

Compliance behavior. Organizations face a significant security emanated from premeditated insider misuse of information systems resources. End users go through stages in order to completed tasks when challenged. Dhillon and Torkzadeh (2006) describe the stages as; awareness regarding the task, intention to towards the task, and actual skills to comply and complete the task. In the context of information security in an organization, attitude of an end-user towards information security controls would reflect the end-user's behavior intention to comply with laid down security policies and procedures (Herath & Rao, 2009; Siponen et al., 2007). When end users utilize any ICT applications during the execution of their everyday activities in the organization, they impliedly come across information security tasks (Kruger and Kearney, 2006). While in the process of performing these information security tasks, end users exhibit a range of information security behaviors such as successful completion of tasks, failure to finish tasks or even failure to initiate tasks that Dhillon and Torkzadeh (2006) describe as behavioral information security. This end user behavior, which is a complex human action that could influence the CIA of information security, is precarious to the realization of information security management efforts in the organization (Da Veiga el al., 2009;

Dhillon & Torkzadeh, 2006; Herath & Rao, 2009; Siponen et al., 2007; von Solms & von Solms; 2005).

Behavior monitoring and compliance are key issues in information security deployment; because to write a policy is one thing, but to be able to enforce it is a totally different thing. Information security researchers have called for close monitoring of insider behavior to ensure compliance with security requirements because most of the crimes committed by insiders are essentially a rational act (Albrechtsen, 2007; Dhillon & Torkzadeh, 2006; Siponen et al., 2010). Von Solms & von Solms; 2005 alluded that it is only when activities are properly monitored that enforcement could be properly enacted.

Deterrent countermeasures. In general deterrence theory, deterrent security countermeasures (e.g., security policies, security awareness programs, and security software) is perceived to be an effective mechanism to regulate information assets misuse in organizations (D'Arcy et al., 2009). Non-compliance behavior is consistent with conclusions in the technology acceptance literature and has been found to have an influence on end user's security behavior (Theoharidou et al., 2005). Deterrence is the process of using fear of punishment, within the parameters of the law, to deter potential wrongdoers from acting. Deterrent techniques such as sanctions and policies are used as reminders to users to allay potential system abuse. The fear of a sanction for policy non-compliance of information security, according to Straub (1990), positively shapes the security behavior of users of information technology.

In order for information security management policies to effective, prospective wrongdoers must be made aware of the consequences for not follow the policies, and this fact must be documented as part of the published policy (Theoharidou et al., 2005). Von

Solms and von Solms (2005) suggest that, failure to prevent or minimize security breaches due to end-user non-compliance is indicators of failed security management.

Information Security Policy

Hone and Eloff (2002) define information security policy simply as a document for the direction of information security inside an organization. It deals with the integrity, availability, and confidentiality of electronic data transmission in the information systems (Knapp et al., 2009). Information security policy could be presented in many forms but the most important process of providing an effective security policy is for it to be in written form (ISO/IEC 17799: 2005). The ISO/IEC 17799:2005 institutes rules and common principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the generally recognized areas of information security management. The ISO/IEC 17799:2005 document covers best practices of control objectives and controls in the following areas of information security management:

- security policy;
- organization of information security;
- asset management;
- human resources security;
- physical and environmental security;
- communications and operations management;
- access control;
- information systems acquisition, development and maintenance;
- information security incident management;

- business continuity management;
- compliance and monitoring.

The ISO/IEC 17799:2005 is a vital element of the general information security management system because it offers the framework for organizations' security implementation agenda (von Solms & von Solms, 2005). In addition, the ISO/IEC 17799:2005 framework provides opportunities for organizations and governments to achieve compliance and reduce the level of security breaches (Knapp et al., 2009). In spite of the widespread recognition in the information systems domain that suitable information security policy may be helpful in providing guidance for protecting valuable data (Bacik, 2008), only few governments in the sub-Saharan Africa countries offer some kind of policy statements dealing with information security (West 2006); Ghana is not an exception.

Information security practitioners today face the challenge of how to present to their larger audience an effective security policy in such a manner that everyone would understand (Doherty & Fulford, 2005). The lack of action on information security policy could be attributed to the unavailability of scholarly studies targeted at information security policies (Knapp et. al., 2009). A Brookings institution sponsored study on global e-Government by West (2008), while about thirty percent of examined sites had some form of privacy policy on their site, only seventeen percent of the sites examined had visible security policy. Table 3 shows statistics of government websites that has some kind of policy statements or documents on them.

Table 3

Government Websites Offering Security Policy

	2001	2002	2003	2004	2005	2006	2007	2008
Privacy	6%	14%	12%	14%	18%	26%	29%	30%
Security	3%	9%	6%	8%	10%	14%	21%	17%

Note: Adapted with permission from “Improving Technology Utilization in Electronic Government around the World,” by D. M. West, 2008, *Brookings Institute*, p. 7. Copyright 2008 by Brookings Institute.

The health care environment today is different from the past decade. The injection of ICTs into the health industry has changed the dynamics of the health institutions to information-intensive such that the nature of data handling has become more delicate and critical (von Solms & von Solms, 2005). Individuals need to know what is anticipated of them in terms of protecting the data they are handling, otherwise they will typically try to act in a way they feel appropriate (Fedor, Carlidwell, & Herold, 2006). Control of information begins and ends with people; from the practitioners who handle the data on a frequent basis, to the policy makers who have the responsibility of creating a comprehensive security policy document for the common good. Without proper direction in the form of written security policy, individuals may inadvertently damage or lose data due to the fact that they may not know how they should properly handle such sensitive data (von Solms & von Solms, 2005).

Information security policies are not designed to only delineate responsibilities and acceptable conduct in an organization (Baker & Wallace, 2007; Doherty & Fulford, 2005), but also to serve as effective deterrents (Straub, 1990). Proper implementation of information security policy as a deterrent could significantly influence the conduct of human behavior in the daily handling of patient data (Von Solms & von Solms, 2005).

Information security policy, a key element of any ISM and other strategies, forms the basis of the action plans and procedures which may lead to operational processes. Identification and implementing an information security policy enhances the ISM framework, which in turn could have a practical significance to health informatics of the e-Government concept. Indeed, the first step towards achieving comprehensive ISM, according to Wood (2005), is to confirm that information security policy is labeled, conserved, and recurrently reviewed. West (2008) contended that formal information security policy is a precondition for a practical information security problem because it necessitates the documentation of exact kinds of information that would need protection.

User awareness and training. To counter the risks posed by inappropriate user action (intentional or unintentional), information security decision makers propose security awareness and education programs for users (Aytes and Connolly, 2004; D'Arcy and Hovav, 2009; Dhillon & Hentea, 2005; Ellof & Ellof, 2005; Knapp et al., 2009; Siponen et al., 2010). Lack of awareness by users indicating the existence of information policies and procedures could hamper overall information security objectives (Knapp et al., 2009). For example, if the users of data in organizations are not cognizant of the existence of information security policy and procedure, it stands to believe that there may be high incidence of data mishandling that could lead to serious security breach.

Consequently, an effective strategic program of policy education is needed to broaden the awareness among organizational participants of the necessity of adherence to information security policy (Ellof & Ellof, 2005). Information security awareness serves not only as a warning sign to users of information security issues (Straub & Welke, 1998), but also as a conduit for users to receive informal training in basic information security concepts (Knapp et al., 2009). Also, information security awareness can serve as a deterrent measure in that end-users would be discouraged from engaging in data misappropriation (Dinev & Hu, 2007). Information security awareness programs such as reminders to change passwords and email messages announcing new virus threats, offer employees the needed skills to help them realize the responsibilities regarding their organizations' information resources, as well as the consequences of noncompliance (D'Arcy & Hovav, 2009).

Besides developing employees' awareness programs, organizations must also recurrently evaluate the needs of their employees and institute education and training programs to that effect (Dhillon & Hentea, 2005). Employees must be made to understand why information security is vital to the success of their organizations. Also, employees must know how they can behave secure. According to Aytes and Connolly (2004), a good information security education and training While education and training are the basis for security management program (Ellof & Ellof, 2005), they don't assurance security conform behavior in daily work life. Education and training would be important for both information systems practitioners and users alike to know the effect of proper information security policies and procedures in order to better preserve data or information (Knapp et al., 2009). Recognizing that security awareness and training programs are designed

largely without proper considerations of users' behavior, Aytes and Connolly (2004) urge organizations to include security behavior of the users in their comprehensive information security management strategy.

Behavior intention. The Theory of Reasoned Action (TRA), a widely applied framework in information systems research (Fishbein & Ajzen 1975), posits that behavior is determined by beliefs about that target behavior via the behavior determinant construct behavioral intentions. The theory predicts that behavioral intentions determinants attitude and subjective norm. Ajzen (1991) further explained that, the influence of the beliefs is captured through behavioral intention factors, subjective norm, and apparent behavioral control (Siponen et al., 2007). Again, the direction of influence is from beliefs, to behavioral intentions and ultimately behavior. The information security literature has begun to highlight the evolutionary, emergent nature of information systems security, particularly from the non-technical perspective. One well recognized view of a non-technical perspective is the organization's climate which incorporates human factors through individuals' observations and descriptions of how an organization is experienced (Kraemer et al., 2009). Colwill (2010) alluded that, human factors focusing particularly on end user perceptions, intentions and behavior are identified as critical elements for understanding how to move forward with information systems security.

Some researchers have recently pointed to awareness as being a central construct in the formation of user behavioral intentions with regard to technologies such as information systems security (Dinev & Hart, 2006; Siponen et al., 2007). The foundational relationship is that an individual must be cognizant or aware of a technology before they can form any beliefs or subsequent behavioral intentions about that technology

(Knapp et al., 2009). Dinev and Hart, (2006) stated that, an individual must be aware of information systems security before one could form beliefs about information systems security; which ultimately lead to behavioral intentions regarding information systems security. In the context of information security policies compliance, a strong behavior intention is an indicative of information security adherence.

Organizational Security Culture

Information security culture is defined as acceptable and often encouraged perceptions, attitudes and assumptions that help protect information assets in an organization (Da Veiga, & Eloff, 2009). According to Schlienger and Teufel (2005), security culture includes both security related beliefs and security related behaviors. The conception of information security culture was comparatively new and was regularly categorized in a simplistic manner (Ruighaver et al.,) till the early part of the century when researchers began to appreciate its importance to the general information security management (von Solms & von Solms, 2005). Information security researchers have long argued that organizations need an organizational security culture in order to comprehensively assurance the security of their information assets (Dhillon & Torkzadeh, 2006; Stanton, Stam, Mastrangelo, & Jolton, 2005). The reason behind the surge in interest in information security culture is attributed to the realization by information systems researchers that the issue of comprehensive information security management goes beyond technical (Stanton et al., 2005) standpoint.

Information security is no different than any other technology and studies have shown that culture has an important impact on the implementation of any new technology or system (Vroom & von Solms, 2004). This is even so because cultural values and

experiences in Ghana are different from those of western developed countries (where most previous ISM research has been located) and therefore require a thoughtfulness of ISM execution.

The most common national cultural model is Hofstede's (2001) framework which classified national culture into five scopes: power distance (a measure of equal distribution of power), avoidance of uncertainty (how uncertain risk threatens cultural members), individualism (the balance between duties and responsibilities), masculinity (how gender is used to separate social roles), and long term orientation (how specific culture influences human and organizational behavior and practices). Hofstede stressed that organizational cultures are embedded inside a national culture and that national culture impacts human practices. As such, the existence of cultural differences regarding the object and use of information and data within e-Government systems suggests that it is important to consider the fit between the various tasks describing different subcultures and the technologies being implemented. The interface amongst these fields of knowledge such as policy and employees behavior has an enormous effect on information security culture, particularly in Ghana where individual rights and privacy are not very much respected as in the western world. Such wanton disrespect to security and privacy cannot be accepted in the health information system and must be changed because the core component of health informatics is to secure patient's data.

Accordingly, to implement an effective informational security policy, the culture of the people must be examined and understood because the goal of a security culture policy is to effect behaviors and actions of the employees or the citizens (in the case of a nation). As employees may have legitimate access to information for their routine

activities, their behavior should conform to ways that would not give rise to a culture where negligence is viewed as an acceptable norm (Da Veiga & Eloff, 2009). It is important for information systems practitioners to remember that the most effective countermeasure is not always the technical measure, but a combination of both technical and non-technical elements.

Top leadership support. Despite that there may be differences in managerial attitudes and perceptions toward security risks that may influence management choices relative to the suitable security actions required, there is a strong theoretical and empirical basis for focusing on the leadership team in the decision-making process (Da Veiga & Eloff, 2009; Knapp et al., 2009; Kritzinger & von Solms, 2005). The idea of leadership support being a necessary condition for successful implementation of ISM is well known (Kritzinger & von Solms, 2005). Involvement is the prominence placed on risk management program by top management as the organization leadership show noticeably support through its own behavior (Da Veiga & Eloff, 2009; Knapp et al., 2009; Kritzinger & von Solms, 2005). Attaining an ample top leadership pledge for cultural change process is the first constituent to information security management. Once management has committed to the new culture, the vision for organization's information security culture should then be incorporated in to the corporate information security policy (Kankanhalli, Teo, Tan, Wei, 2003; Knapp et al., 2009).

Normative beliefs. The role of social influence in terms of normative beliefs, subjective, peer and descriptive norms in information systems research has been considered for some time now (Herath & Rao, 2009). While the information systems literature has used variety of tags for subjective norm concepts, each of these concepts

contain the notion that the individual's behavior is influenced by what the relevant others expect them to do (Da Veiga & Eloff, 2009). The understanding that persons are more likely to conform with significant others' prospects when those others have the ability to reward the desired behavior (Kritzing & von Solms, 2005). Venkatesh et al. (2003) posited that social impact in information technology acceptance is intricate and could be contingent on variety of conditional effects as well.

Fishbein and Ajzen (1975) stated that intention greatly influences an individual's behavior, and behavioral change is ultimately the result of changes in normative beliefs (Ajzen, 1991); which is based on whether or not an important individual requests the person to perform the behavior in question. As regards to information security management, normative beliefs may arise due to an organizational culture. Without information security mechanisms to direct and influence employee conduct, employees could well relate with information assets in manners that would lead to risky behavior (Herath & Rao, 2009; Knapp et al., 2009; Kritzing & von Solms, 2005). If action is not taken in time, this potentially harmful behavior could unfortunately give rise to a culture where neglect is regarded as acceptable (Ajzen, 1991; Kritzing & von Solms, 2005; Venkatesh et al., 2003).

Summary

This chapter reviewed the relevant literature pertaining to the non-technical security management elements of information security and health informatics. Information security is a major concern in health informatics given that large volumes of proprietary data are processed every second in the healthcare industry. Studies were reviewed that showed tremendous recognition of the importance of management of

information security, which has the ultimate goal of designing and implementing effective information security strategies (Chang & Lin 2007). There is an overall consensus among researchers that non-technical elements such as organizational culture, security policies, and human behavior actions are of benefits for a wide range of information security (Colwill, 2010). Studies by Vroom and von Solms (2004), Knapp et al., and Siponen et al, (2007) show the relationship between information security and organizational culture. Also monitoring and compliance of policies are other key issues in information security implementation (Doherty & Fulford, 2005; Von Solms & von Solms, 2005) that was researched in to.

In contrast, there are few quantitative studies on information security practices that integrate all components of as a means to achieve effective security control. According to Alfawaz, et al., (2010), most of the information security researches conducted to date have been on specific issues (culture, policy, management support etc.) only; as against to the entire issues collectively. It is likely that this dearth of research into comprehensive information security management is the result of the perception that, from the perspective of some researchers, such studies would appear to be methodologically weak. Nevertheless, information security practitioners should consistently view information security components holistically and design their security strategies around as such.

Information has and will continue to be seen as an extremely important asset in today's business environment (Chang & Lin, 2007; Da Veiga & Eloff, 2009; Doherty & Fulford, 2005; Siponen et al., 2009). It is therefore important for organizations to recognize the serious need to holistically manage and secure its information assets like it would any other valuable assets (ISO/IEC 27002, 2005). It is also important that every

member of the organization recognize that they play a role and share responsibility for the organization's information security effectively. Failure to recognize the importance of non-technical security components could have a negative impact on an organization's information security blueprint implementation (West, 2006).

Chapter 3: Research Method

The purpose of this non-experimental quantitative study was to examine the impact of the non-technical security management factors including organizational culture (leadership support and normative beliefs), security policy (user awareness and behavior intention), and human behavioral actions (deterrent countermeasures and compliance behavior) on information security management in health informatics. This chapter represents the research methodology section of the study including method and technique used in probing the lack of non-technical security management measures in the formulation of information security management (ISM) in health informatics. In addition, the operational definition of the variables, the data collection, processing and analysis, the methodological assumptions, limitations and delimitations were presented. The research design was impacted by the findings of the literature review presented in Chapters 2. To evaluate the influence of non-technical factors on information security in the healthcare industry of Ghana, the following research questions were presented, together with null hypotheses (H_0) and alternative hypotheses (H_a) as they were associated with each research question:

RQ1: To what extent (if any) is there a relationship between security policy, as measured by user awareness and behavior intention, and Information Security Management, as measured by confidentiality, integrity, and availability?

RQ2: To what extent (if any) is there a relationship between organizational culture, as measured by leadership support and normative beliefs, and

Information Security Management, as measured by confidentiality, integrity, and availability?

RQ3: To what extent (if any) is there a relationship between human behavior actions, as measured by compliance behavior and deterrent countermeasures, and Information Security Management, as measured by confidentiality, integrity, and availability?

RQ4: To what extent (if any) do non-technical security management factors of security policy (measured by user awareness and behavior intention), organizational culture (measured by leadership support and normative beliefs), and human behavior actions (measured by compliance behavior and deterrent countermeasures) predict Information Security Management (measured by confidentiality, integrity, and availability)?

The following hypotheses were generated in order to answer and analyze the research questions of the study:

H1₀: There is no statistically significant relationship between security policy as measured by user awareness and behavior intention, and Information Security Management, as measured by confidentiality, integrity, and availability.

H1_a: There is a statistically significant relationship between security policy as measured by user awareness and behavior intention, and Information Security Management, as measured by confidentiality, integrity, and availability.

- H2₀:** There is no statistically significant relationship between organizational culture as measured by leadership support and normative beliefs, and Information Security Management, as measured by confidentiality, integrity, and availability.
- H2_a:** There is a statistically significant relationship between organizational culture as measured by leadership support and normative beliefs, and Information Security Management, as measured by confidentiality, integrity, and availability.
- H3₀:** There is no statistically significant relationship between human behavior actions as measured by compliance behavior and deterrent countermeasures, and Information Security Management, as measured by confidentiality, integrity, and availability.
- H3_a:** There is a statistically significant relationship between human behavior actions as measured by compliance behavior and deterrent countermeasures, and Information Security Management, as measured by confidentiality, integrity, and availability.
- H4₀:** The non-technical security management factors of security policy, organizational culture, and human behavior actions, do not significantly predict Information Security Management, as measured by confidentiality, integrity, and availability.
- H4_a:** The non-technical security management factors of security policy, organizational culture, and human behavior actions, are significantly

predictive of Information Security Management, as measured by confidentiality, integrity, and availability.

Research Methods and Design

This study employed a quantitative design and descriptive correlational methods to test the hypotheses and answer the research questions. Trochim (2006) defined quantitative research as a process of inquiry examining an identified problem that is based on testing a theory measured by numbers and analyzed with statistical techniques. Brady and Collier (2004) provided a more technical definition of mainstream quantitative methods as a tactic to methodology that is strongly oriented toward regression analysis, econometric refinements on regression, and the search for statistical alternatives to regression models in contexts where specific regression assumptions are not met. The econometric refinements and statistical alternatives referred to by the authors, although are beyond the scope of this chapter, include logit and probit models, time-series analysis, and a variety of techniques to circumvent problems that can occur in regression analysis, such as heteroskedasticity and autocorrelation (Brady & Collier, 2004 ; Trochim & Donnelly, 2007).

Largely, quantitative methods have played a major role in improving on commonly used research tools within the structure of regression models that are often used in the field of business research (Trochim, 2006). The goal of quantitative research is to examine particular instances or aspects of phenomena to determine if predictive generalizations of a theory hold true or to test causal hypotheses (Creswell, 2009). Quantitative researchers are much more likely than their colleagues to base their designs on the logic of experiments (Trochim & Donnelly, 2007). For instance, quantitative

researchers often emphasize control groups, pretests, and other elements that provide them with the opportunity to hold some factor(s) constant in their attempt to make causal inferences. In quantitative studies, sampling is based on the logic of probability to produce statistical representativeness (Creswell, 2009). Additionally, in quantitative research, sampling is done before the data are collected. Quantitative methods are fundamentally a distinction of research techniques that are used to collect quantitative data (Trochim, 2006).

There are three key criticisms of quantitative research that are discussed here. First, some critics argue that in quantitative studies, all cases are treated as though they are alike since research methods were adopted from the physical sciences (Martens, 2005) and that people can simply point diverse connotations to something even when they are feeling the same occurrences. Related to the first is the criticism by certain researchers that that quantitative methods are integrally biased. According to those critics, quantitative methods fail to take into account the exclusive cultural roots and other serious characteristics of sidelined groups of people (Westerman, 2006). Thus, the usage of quantitative methods may not be suitable when it comes to populations that have been politically excluded. The third criticism of quantitative research methods is that, by taking individuals out of their usual locations to examine the inadequate features of what a person thinks or believes (Teddlie & Yu, 2007), it would be difficult to fully comprehend the true connotation of actions or answers.

Accordingly, a number of statistical analyses steps were used to evaluate the study objectives. The statistical analyses steps are detailed as follows:

Data screening. Data were screened for quality and an excess of missing responses. Items and cases with an excess of missing responses were removed. Also, ambiguous responses were individually inspected, and removed or recoded appropriately.

Description of the sample. Frequency and percentage data were tabulated in order to characterize the sample in terms of gender, age, profession, education, and experience.

Descriptive analysis of survey items. The mean, standard deviation, and distribution of responses for each survey item were calculated.

Relationship amongst survey items. Pearson product moment correlation coefficients were computed to evaluate the item inter-correlations within each section of the survey.

Reliability of survey sections. Reliability statistics were calculated for each section of the survey, to determine the internal consistency of the items. Cronbach's alpha is calculated from the average inter-item correlations of items and provides an indication of the internal consistency of the items. Higher values of alpha are desired and indicate greater reliability of the composite. Item-total scale reliability statistics were also calculated to evaluate the contribution of each of the items to the scale, including: corrected item-total correlations (correlation of the item with the summated score for the other items), squared multiple correlation (predicted variance in the item obtained by regressing the individual item on the remaining items) and Cronbach's alpha with item removed (the scale's Cronbach's alpha reliability coefficient for internal consistency if the individual item is removed from the scale). The following rules of thumb provided by George and Mallery (2003) were used to evaluate the Cronbach's alpha values: $> .9$ –

Excellent, > .8 – Good, > .7 – Acceptable, > .6 – Questionable, > .5 – Poor, and < .5 – Unacceptable (p. 231).

Item recoding. Negatively worded items on the survey were identified via the correlations and reliability results. That is, agreement with these statements was reflective of the opposite sentiment to the remaining items within a section. Negatively-worded items were reverse-coded (i.e., a score of 5 was re-coded to a score of 1, etc.) prior to the creation of composite scores (i.e., section and sub-domain means). This was conducted to ensure that scores were not created by averaging across positive and negative items, thereby cancelling out any effects.

Creation of composite scores. Composites for each sub-dimensions and section of the survey was computed by taking the arithmetic mean of the constituent items. Where identified in the reliability analysis, some of the item scores were reverse.

Descriptive statistics of composite scores. The mean, standard deviation, and distributional statistics (e.g., skewness) of the composite scores (i.e., section and sub-domain means) were calculated. Boxplots of the composite scores were produced to visually inspect the distributions for gross deviations from normality or the presence of outliers. Outliers were also assessed by creating standardized scores (i.e., Z scores) for each of the variables. Z scores with values greater than $Z \pm 3.29$ ($p < .001$) were considered univariate outliers and were removed from the analysis.

Multivariate screening. Multivariate outliers are cases with an unusual pattern of scores on two or more variables. To screen for multivariate outliers, Mahalanobis distances were calculated for each pairing of IV and DV, and for the combination of the three IVs with the DV. Mahalanobis distance is the distance of a case from the centroid of

the remaining cases where the centroid is the point created by the means of all the variables (Tabachnick & Fidell, 1996). Mahalanobis distances are evaluated against the chi-square distribution with the degrees of freedom equal to the number of variables in the analysis. A probability estimate of $p < .001$ was used for a case being a multivariate outlier.

Relationship amongst section and sub-domain scores. Pearson product-moment correlation coefficients were computed between the dependent variable of Information Security Management and the independent variables of security policy, organizational culture, and human behavior actions. Furthermore, correlations were calculated between the sub-domain scores of each variable. The results are presented according to the research questions, and were used to address whether there was a statistically significant relationship between the variables under study. Cohen's (1992) effect size conventions were used to evaluate the size of the relationships: $r = .1$ – small, $r = .3$ – medium, and $r = .5$ – large.

Bivariate, multiple and multivariate regression analysis. A number of regression procedures were used to clarify the relationships between the study variables. Bivariate regression was used for each research question, to determine to what extent there was a relationship between the predictor and each of the criterion variables (i.e., what percentage of variance was explained). In each research question, analyses were undertaken to investigate the contribution of the sub-domain scores to the overall effect. This was accomplished using multivariate multiple regression. The three sub-domains of ISM (i.e., confidentiality, integrity, and availability) were the dependent variables (DV) or criterion variables. The sub-domain scores of the independent variable (IV) relevant to the

particular research question served as the predictors. The multivariate effects were evaluated to determine whether each IV sub-domain was a significant predictor of the group of DV sub-domains. The between-subjects effects were evaluated to determine whether each DV sub-domain was significantly predicted by the IV sub-domains.

For each regression analysis, examination of the histograms of the residuals and the scatterplots of the residuals versus predicted values provided a test of the assumptions of normality, linearity, and homoscedasticity between predicted DV scores and errors of prediction (Tabachnick & Fidell, 1996). The histogram of the standardized residuals should follow a normal distributional pattern, indicating good adherence to this assumption of linear regression. The scatterplot of the standardized residuals versus predicted values are used to evaluate normality, linearity, and homoscedasticity. Normality and linearity in the residuals scatterplot are indicated by even numbers of values above and below zero across the range of possible values, without any apparent “curvature” in the graph, or increasing/decreasing values. Heteroscedasticity would be indicated by varying dispersion of the residuals at different predicted values. For example, the residuals could become more widely dispersed as the fitted value increased. The residual statistics were calculated and examined using SPSS for each regression analysis. There were no violations of the assumptions of normality, linearity or homoscedasticity. As such, these results are not discussed in detail within this chapter.

All analyses were conducted using SPSS v.20. Charts were created using SPSS v.20 or Microsoft Excel 2010. An alpha level of .05 was used as a decision point for statistical significance.

Participants

The sampling frame of this study was healthcare professionals from the Korle-Bu Teaching Hospital (which include physician consultants, surgeons, anesthetists, pharmacists, nurses/midwives, pathologists, radiologists, and laboratory technologists), and technocrats from the Ministry of Health. While the health professionals were selected because they would be the principle users of e-Health/Health Informatics, the technocrats were included because in addition to being the policy makers, these officials are more knowledgeable in the development of and implementation of Health Informatics/e-Health in Ghana. Their direct contribution could have an enormous bearing on the results of the survey. The criterion determined appropriate for identifying participants for this study include (a) continuous employment (any capacity) at Korle-Bu Teaching Hospital in Ghana and (b) an official from the ministry of Health knowledgeable with Ghana's e-Health concept since the planning and implementation phase of Ghana's ICT in 2004.

Researchers apply diverse methods and measures to determine an adequate sample size when conducting surveys. In this study, 200 healthcare professionals and stakeholders were purposely selected to partake in the survey. To determine the minimum sample size for this study, the G*Power 3.13 statistical analysis software was used to perform a priori analysis (Faul et al., 2007). Applying a one-tailed test at a significance (alpha) level of .05 with an effect size of 0.30, and a confidence level of 90% (Price et al., 2005), a minimum sample size of 56 participants were needed to examine the impact of non-technical components of security measures on comprehensive management of information security. This sample size represents a sizeable manpower at Korle-Bu Teaching Hospital and as well as the Ministry of Health. With an expected response rate

of 31.4% (Ganczarski, 2006) and a sample size of 56, the minimum number of surveys to be distributed is 116. However, to maximize the number of completed surveys, a total of 200 surveys were distributed.

A purposive sample of healthcare stakeholders (health professionals and technocrats) from Korlr-Bu Teaching as well as the Ministry of Health. Purposive sampling, which often uses nonprobabilistic samples, is field oriented and not concerned with statistical generalizability (Teddlie & Yu, 2007). The aim of purposive sampling is to assist the researcher in getting a range of illuminative ideas from information-rich cases allowing the researcher to obtain a painstaking empathetic of the phenomenon (Martens, 2005). Purposive samples are selected based on a prearranged benchmarks associated with the research (Martens & McLaughlin, 2004). It is incumbent upon researchers to conduct a thorough literature review to understand the “edge of the field” and whether the study population or question is a new or is significant contribution. In this study therefore, purposeful sampling was considered because of lack of a reliable data as a result of the absence of a comprehensive information security management in the country’s overall ICT strategy.

The survey was hand delivered (drop-off) because such data collection method usually has a high response rate as researchers can make direct contact with participants, who may have their follow up questions or queries answered (Trochim, 2006). While the response rate for most surveys are declining, the response time for drop-off is still above seventy percent (Cull, O'Connor, Sharp, & Tang, 2005). Another reason for opting the drop off method was that it is more cost effective when compared to direct mail or online. Participants were provided with introductory letters describing the research and an

Informed Consent Form as the first page of the survey. The information obtained in this dissertation was treated as strictly confidential unless otherwise required by law. As an enticement to participate in the survey (Baker & Wallace, 2007), a copy of the results will be sent to each participant who so wishes.

Materials/Instruments

Deployment of research methods such as surveys and the validation of frameworks and questionnaires have long been used in the information security domain (Schlienger & Teufel, 2005). According to Leedy and Ormrod (2005), a research tool is a specific mechanism or strategy the researcher uses to collect, manipulate or interpret data. The research instrument for this study was a combination of three previously used and validated instruments adopted from ISCF (Sipoen et al., 2010; see Appendix C), ISMC (Chang & Lin, 2007; see Appendix D), and ISGF (Da Veiga & Eloff, 2009; see Appendix E). The rationale for adopting pre-tested validated instruments from previously published studies was because it improves the reliability of the results (Herath & Rao, 2009). Permissions to use the instruments were granted by the respective authors (see appendix C, D and E).

The ISCF by Siponen et al., (2010) was developed from the human security clause of the ISO/IEC 17799 Standard subsection to examine the relationship between rewards and actual compliance with information security policies. The authors found that deterrents, information quality and normative beliefs have significant effect on intention to comply and actual compliance of information security policies. Using a rigorous development and validation procedure, the authors ensured that the ISCF questionnaire

have adequate internal consistency and reliability as measured by a Cronbach's alpha coefficient of 0.859.

Chang and Lin (2007) developed the ISMC to examine the influence of organizational culture on the effectiveness of implementing information security management (ISM). In order to achieve that, the authors formulated a model of the relationships between information culture and ISM. They found out organizational culture traits of effectiveness and consistency, have strong effect on ISM. Chang and Ling (2007) conducted reliability check of the constructs using Cronbach's alpha coefficient. All three ISM determinants of confidentiality, integrity, and availability (CIA) recorded 0.815, 0.717, and 0.673 respectively; very significant.

The ISGF construct was developed by Da Veiga and Eloff (2009) to examine approaches (ISO/IEC 17799-2005; PROTECT, 2005; CMM, 2001; ISA, 2000) towards information security governance frameworks in order to arrive at a completed list. Da Veiga and Eloff (2009) used a variation of the ISGF surveys, and conducted a principle component analysis (PCA) in which convergent and discriminant validity in all constructs were established. Additionally, the authors' use of measurement scales indicated acceptable reliability coefficients as measured by Cronbach's alphas of 0.918.

The survey instrument for this study was designed to test the correlational relationships between the dependent variable (information security management) and the independent variables (organizational culture, security policies, and human behavior actions). The survey instrument was based on five-point Likert-type scale responses in the following order of scale: 1= *strongly disagree*, 2= *disagree*, 3= *neutral*, 4= *agree*, 5= *strongly agree*. When variables are related to survey instrument items in a study, it helps

the researcher in expressing how the research questions were framed and analyzed (Creswell, 2009).

Although prior validation of the study constructs may be thorough but because this study instrument was adopted from a combination of previously developed instruments in to being from different study context, the need for additional validation and reliability for the instrument was necessitated (Tung, Chang, & Chou, 2008). As required when a research involves human subjects, the author obtained permission from the Institutional Review Board (IRB) of Northcentral University before even the pilot test begun. A pilot test of the combined questionnaire was conducted prior to the main study ensure that the selected questionnaire epitomize the concept around which the study was based on.

A panel of *experts* comprising two information systems professors and a cardiologist were empaneled to appraise the construct and offer their suggestions (if any). The reason for the inclusion of a medical doctor in the panel in particular was to delimit bias error in the research questions. Using a panel of experts to review the test specifications and the selection of items can improve the content validity of a test (Anastasi & Urbina, 1997; Foxcroft, Patterson, Le Roux, & Herbs, 2004). Among the terms of reference for the *experts* were the appraisal of the study and then note on whether the contents cover a demonstrative sample of information security management domain, identify ambiguities and difficult questions, and the time taken to complete the questionnaire. The panel of *experts* largely agreed that the study contents is indeed expressive of information systems/security domain. They however suggested that the number of questionnaire should be reduced to avoid the probability of premature termination or other behavior patterns from exhaustion. Buoyed by the feedback and

recommendations from the experts, the author removed ambiguities of terms being used to protect respondents' anonymity prior to the start and during the survey process. The questionnaire was also scaled back from 50 to 35.

Data from the pilot study were not included in the data for the actual research project. Study participants were encouraged to truthfully divulge what they thought about the subject matter. In order to maintain the privacy of the participants, names and addresses of the respondents were written or typed on the back of the envelopes. Furthermore, all identifiable characteristics from the interview data were removed. Finally, since English is the official language of Ghana, neither the survey questionnaires nor the interview process would need to be translated.

Operational Definition of Variables

Trochim and Donnely (2007) defined operationalization of study variables as the process of translating an idea or concept into reality. Operationalization, Singleton and Straits (2005) explained, provides the specifics about the variables in a study. The independent variables for the study were organizational culture, security policy, and human behavior actions. The dependent variable was information security management.

Human behavior actions. Human behavior actions refers to a situation that, while in the process of performing these information security tasks, end users exhibit a range of information security behaviors such as successful completion of tasks, failure to finish tasks or even failure to initiate tasks that Dhillon and Torkzadeh (2006) describe as behavioral information security or human behavior actions. This end user behavior, which is an intricate human action that could influence the *CIA* of information security, is critical to the success of information security management efforts in the organization (Da Veiga et

al., 2009). Deterrent security countermeasures (e.g., security policies, security awareness programs, security software) used by organizations in order to influence the effect that a threat has on their information systems in order to reduce risk and increase information systems effectiveness (Siponen et al., 2007). As applied in ISM, the goal of deterrent efforts is to provide disincentives for would-be computer abusers (D'Arcy & Hovav, 2009). Compliance behavior refers to extent that end users would go in order to comply with information security policies (Siponen et al., 2010). Countless organizations identify that their employees, who are often considered the *weakest link* in information security, can also be great assets in the effort to reduce risk related to information security (D'Arcy & Hovav, 2009). Factors such as subjective norms, peer behaviors, deterrence, and training influence employee information security behavior; which in turn is related to information security management. Since employees who comply with the information security rules and regulations of the organization are the key to strengthening information security, understanding compliance behavior is crucial for organizations that want to leverage their human capital (Dhillon & Torkzadeh (2006).

In this study, human security actions, an independent variable, was measured by compliance behavior and deterrent countermeasures using a Likert-type scale of 1-5 scale ranging from strongly agree, agree neutral, disagree, and strongly disagree. The variable was measured using 8 questions (28-35) adopted from Siponen et al. (2010).

Information security management. Information security management is defined as structured process for the implementation and ongoing management of an information security program in an organization (ISO/IEC 17799: 2005). Real security can be achieved when employees of the organizations collaborates and behave in a way that

could compromise the core principles of information security; confidentiality, integrity and availability (CIA). Confidentiality means that only authorized parties can access computer related assets (ISO/IEC 17799: 2005). The term integrity refers to the state in which electronic assets can be modified only by authorized parties or only through authorized means (ISO/IEC 17799: 2005). Availability in this context refers to how accessible assets are to an authorized party at appropriate time (ISO/IEC 17799: 2005).

In this study, information security management (the dependent variable) was measured by the CIA (confidentiality, integrity, availability) principles based on the Likert-type of 1-5 scale ranging from strongly agree, agree, neutral, disagree, and strongly disagree, using survey questions 6-11 from the survey instrument (see Appendix E) adopted from Chang and Lin (2007).

Organizational culture. Organizational culture is the beliefs and values that have existed in an organization for a long time, and to the beliefs of the employees and the anticipated value of their work that will influence their attitudes and behavior. Several information security researchers have found that organizational culture is significantly correlated with leadership behaviors and job satisfaction, and also leadership behaviors was significantly correlated with job satisfaction (Herath & Rao, 2009; Siponen et al., 2009). Top leadership support is decisive to employee attitude towards information security (Knapp et al., 2009). Leadership usually adjusts their behavior to accomplish the mission of the organization, and this could influence the employees' overall actions. Much of the research in information systems has considered the role of social influence in terms of normative beliefs (Da Veiga & Eloff, 2009). Normative beliefs are individuals' beliefs about the extent to which other people who are important to them think they should

or should not perform particular behaviors. As top leadership adjust their behavior, they indirectly influence the behavior of employees therefore normative beliefs may arise due to an organizational culture.

Thus in this study, organizational culture, which is an independent variable, was measured by leadership support and normative beliefs based on Likert-type scale of 1-5 ranging from strongly agree, agree, neutral, disagree, and strongly disagree using survey questions 20-27 from the survey instrument (see Appendix E) adopted from Siponen et al. (2010).

Information security policy. Information security policy is a control documents or statements concerning security that are formally defined and approved by an organization; security policies reflect the intent of the organization (Da Veiga & Eloff, 2009). Security policies provide guidelines and management advice for improving information security. Information security policy, a key element of any ISM and other strategies, forms the basis of the action plans and procedures which may lead to operational processes. Users require understanding, learning, acquiring skills, and using the obtained knowledge, of which the latter is critical to the success of organizational security policy (Knapp, 2009). For security policy to be effective everyone from the organization must be able to access the knowledge pertaining to security measures, practices and procedures and all efforts shall be made in building confidence in information systems (Puhakainen, 2006). Security awareness efforts are designed to change behavior or reinforce good security practices. Behavior intention to comply with behavior is assumed by many researchers to be the key predictor of behavioral performance. Person's intention to perform a certain behavior is assumed to be

determined by the person's attitude, subjective norm, and behavioral and normative belief (Siponen et al., 2010). Users' intentions to comply with information security policies may be based on the stimulated behaviors of their bosses or peers in the organization.

In this study, security policy, an independent variable, was measured by user awareness and behavior intention to comply based on Likert-type scale of 1-5 ranging from strongly agree, agree, neutral, disagree, and strongly disagree using survey questions 12-19 from the survey instrument (see Appendix E) adopted from Siponen et al., (2010).

Data Collection, Processing, and Analysis

This study was conducted using the quantitative method approach. Permission was obtained from the Institutional Review Board (IRB) of Northcentral University before data were collected. Researchers have different ways of administering surveys, which are commonly divided into two categories: interview-based and self-completed (Leedy & Ormrod, 2005). Regarding the quantitative data collection process, I personally dropped-off and hand collected the survey from the sites. The drop-off method was chosen (instead of online/internet based method) in order to avoid problems associated with the limited access to internet in Ghana (Williams & Boren, 2008). For a start, an informed consent forms providing a brief description of the study and emphasizing confidentiality was included and participants agreed and signed off the forms before they could participate in the survey process. Data collected from the survey was integrated for processing using Microsoft Excel spreadsheet, which was then uploaded into Statistical Package for Social Sciences (SPSS) software for the analysis of the hypotheses associated with the data into meaningful information.

Multiple linear regressions analyses were used to analyze the data collected from the survey. The analyses were based on the dependent variable (information security management) and the independent variables (organizational culture, security policy, and human behavior actions). The use of both SPSS and Microsoft Excel software stems from the fact that, while the SPSS helped running the statistical tests, the Excel provided better user friendliness and better graphics capabilities.

Methodological Assumptions, Limitations, and Delimitations

Every research study will intrinsically encounter some limitations (Mathie & Carnozz, 2005) and so the limitations expected in this study are consistent with several research limitations. The limitations included in this study are the sample population size and the quality of both the questionnaire and the information to be collected from the survey. While findings of this research may be similar to some of the previous studies (Shanks, 2006), they may not be generalized in all cases due to many reasons. The sample population used in this population may suffer from the deficiency of generalizability as the number participants used in the study were far less than adequate representation of the study population. For example, while the study is meant to cover the entire healthcare industry in Ghana, the sampling population for this study covers only one hospital and one ministry in Ghana.

Thus the results of the study may not accurately reflect the true situation of information security management of the entire healthcare industry in Ghana. Another limitation is the quality of the information. The quality of information could be affected by a systematic error (Mathie & Carnozz, 2005) which could threaten the validity of the study. For example, respondents' error and bias in the self-administered survey, such as

exaggerations, inaccurate recall, or entirely not forthcoming, may affect the findings of the study. Finally, the main delimiting factor for this study is the cost involved in gathering the data from Ghana. The cost of flying in and out, accommodation and logistics is insurmountable such that the researcher may not be able to stay long enough or fly back for follow up questions. However, these limitations should not be considered as key threats to the study because I had already anticipated these kinds of issues and every effort was made to mitigate them.

Ethical Assurances

The research methods used in this study followed all the basic ethical principles of research per The Belmont Report: respect for persons, beneficence, and justice (The Belmont Report, 1979). The major stakeholders operating in the country: the ministry of health and the healthcare professionals (doctors, pharmacists, nurses, etc.), and the administrators of the various healthcare facilities/institutions would be accorded the required respect. All stakeholders were provided with sufficient information, and may choose to voluntarily participate or not to. Participants did not encounter any physical, psychological, or reputational risks during the course of conducting this study. Similarly, there were no reputational, physical or psychological risks for the respondents because of participating in the envisioned study. Participants were informed that they could withdraw from the study at any time without any problems for withdrawal.

In the course of data collection, no data was obtained from vulnerable groups such as children. Therefore these vulnerable groups were not put in harm's way, and there were no misleading action undertaken to gather data. Furthermore, no sensitive personal information was collected that would be injurious to any participant, and there were no

insidious interventions undertaken in this study. I was not aware of concierges that would need to be contacted to gain access to the respondents during the course of the study. If concierges were encountered, the information gained from these concierges would be minimal and no personal information beyond that necessary, such as names and phone numbers, would be collected. In the end, the information collected will be immediately destroyed after the purpose for which the data was collected had been served.

Summary

This chapter contains an in-depth discussion of the appropriateness of the research design, the research question, the population, the process of obtaining informed consent from the participants, the sampling frame, the procedures to maintain confidentiality, the geographic location where the study will take place, the instrumentation, data collection, data analysis, and the validity and reliability of the data to be collected. The problem addressed in this study was the lack of non-technical security management measures in the formulation of ISM by the stakeholders in health informatics in Ghana. In this study a quantitative design and descriptive correlational methods was employed to test the hypotheses and to probe the underlying issues such as why there is the lack of recognition of a comprehensive information security management as an essential part of health informatics implementation in Ghana.

The population selected for this study was the stakeholders in Ghana's healthcare industry. Data was collected by means of a drop-off survey. The questionnaire for the study was based on pre-validated instruments by Siponen et al., (2007), Da Veiga and Eloff (2009), and Chang & Lin (2007). Multiple linear regressions were used to determine any relationships between information security and the salient variables.

Findings from the survey were discussed in detail in chapter four. Finally, the chapter covers important assumptions as well as all ethical rules and guidelines to be strictly followed in this study.

Chapter 4: Findings

The purpose of this non-experimental quantitative study was to examine the impact of the non-technical security management factors including organizational culture (leadership support and normative beliefs), security policy (user awareness and behavior intention), and human behavior actions (deterrent countermeasures and compliance behavior) on information security management in health informatics.

The instrument for this study was combined from three previously used valid and tested instruments developed from the ISO/IEC 27002 Standard. The ISMC (Chang & Lin, 2007), the ISGF (Da Veiga & Eloff, 2009), and the ISCF (Sipoen et al., 2010) were used to measure the relationships information security management, security policy, organizational culture, and human behavior actions, and their sub-dimensions. The sample for this study was drawn from the population of healthcare professionals, ICT and e-Government technocrats in Ghana.

This chapter contains the results obtained from the statistical analysis of the survey data, and evaluation of the research questions. First the statistical methodology used to analyze these data is described. Descriptive statistics are then presented in order to characterize the demographic nature of the sample. The responses to each of the items on the survey are presented, and analyses related to the reliability of the sections of the survey are discussed. The section and sub-domain scores are also described and evaluated. Following these descriptive analyses, each of the research questions was addressed in turn. The statistical methods used to evaluate the research questions are presented, the results of the analyses are evaluated, and decisions regarding the hypotheses

are made. The chapter ends with an evaluation of the findings in the context of the literature.

Results

Data screening. There were 177 respondents out of the 200 surveys that were dispersed in this study. Items and cases with an excess of missing data revealed complete data for all cases on the non-demographic survey items. Missing data were present on the variables of age ($n = 4$), education ($n = 10$), and years of experience ($n = 15$).

Description of the sample. The demographic characteristics of the sample are shown in Table 4 and Appendixes H,I,J, K, and L. The sample was predominately male, with 63% males and 37% females. In terms of the age of respondents, 19% were between 30 to 40 years, 32% were between 41 to 50 years, 33% were between 51 to 60 years, and 15% were over 60 years. Four respondents did not provide their age group. The professions of respondents were 20% physicians, 22% pharmacists, 18% nurses, and 20% public servants or government officials. A further 20% of the sample was “other” professions. Regarding level of education, 13% had advanced level/HND education, 33% had bachelor’s degrees, 24% had master’s degrees, and 24% had doctorates. Ten respondents (6%) did not provide a valid response to this question. There were 11% of respondents with less than one year of experience with health informatics, 23% with one to three years of experience, 30% with four to five years of experience, and 28% with more than five years of experience. Fifteen respondents (9%) did not report their years of experience.

Table 4

General Demographic Characteristics of Respondents

Variable	Values	Frequency	Percent
1. Gender	Male	112	63.3
	Female	65	36.7
2. Age group	30-40 years	33	18.6
	41-50 years	56	31.6
	51-60 years	58	32.8
	Over 60 years	26	14.7
	(Missing)	(4)	(2.3)
3. Profession	Physician	36	20.3
	Pharmacist	39	22.0
	Nurse	32	18.1
	Public Servant or Gov. Official	35	19.8
	Other	35	19.8
4. Education	Advanced Level/HND	23	13.0
	Bachelor degree	59	33.3
	M.A./M-phil. or MBA	42	23.7
	PhD or Ed.D	43	24.3
	(Missing)	(10)	(5.6)
5. Years of experience	Less than 1 year	19	10.7
	1-3 years	41	23.2
	4-5 years	53	29.9
	More than 5 years	49	27.7
	(Missing)	(15)	(8.5)

Description of variables. This study consisted of one dependent variable (DV) and three independent variables (IVs), each with sub-dimensions. The dependent variable – Information Security Management (ISM) – was measured by three sub-dimensions (confidentiality, integrity, and availability) comprised of two items each. The three IVs each contained two sub-dimensions, measured by four items each. These variables, their sub-dimensions and corresponding survey items are summarized in Table 5 (see Appendix G for survey items). Each item was rated on a five-point Likert-type scale with the following response options and corresponding assigned numeric codes: Strongly Agree (5), Agree (4), No Opinion (3), Disagree (2), Strongly Disagree (1). Thus, higher scores indicated more agreement with the items.

Table 5

Description of Variables in This Study

Type	Variable	Dimensions	Survey Items (No.)
DV	Information Security Management	Confidentiality	6-7 (2)
		Integrity	8-9 (2)
		Availability	10-11 (2)
IV	Security Policy	User Awareness	12-15 (4)
		Behavior Intention	16-19 (4)
IV	Organizational Culture	Leadership Support	20-23 (4)
		Normative Beliefs	24-27 (4)
IV	Human Behavior Actions	Compliance Behavior	28-31 (4)
		Deterrent	32-35 (4)
		Countermeasure	

Note. DV = dependent variable, IV = independent variable.

Information security management (ISM) – dependent variable. Information Security Management (ISM) was the dependent variable in this study, and was measured by three dimensions: Confidentiality, integrity, and availability. The distribution of responses to the items within this construct is shown in Table 6. The means for the items are also shown. Each of the means fell between scores of '3' and '4', corresponding to response options of 'No opinion' and 'Agree', respectively. The highest mean ($M = 3.95$) in this section was for the item within the Availability sub-domain: "There are well established information access control procedures in my organization..." The lowest mean was for the item within the Integrity sub-domain: "My organization regularly updates information resources and constantly creates backups", with a mean score of 3.67.

Table 6

Item Responses for Information Security Management

Item	Mean (SD)	<u>Distribution of Responses</u>				
		5	4	3	2	1
<i>Confidentiality</i>						
My organization enforces security controls (firewall, anti-virus, encryption, etc.) to protect sensitive information. (CONFID1)	3.91 (1.07)	56 (32%)	80 (45%)	16 (9%)	19 (11%)	6 (3%)
My organization has well implemented security practices to protect important information from being stolen by malicious intrusions (such as break-in, Trojans, and spy-wares). (CONFID2)	3.94 (1.12)	66 (37%)	65 (37%)	26 (15%)	10 (6%)	10 (6%)
<i>Integrity</i>						
My organization regularly updates information resources and constantly creates backups. (INTEG1)	3.67 (1.20)	50 (28%)	62 (35%)	34 (19%)	18 (10%)	13 (7%)
My organization has change management control in place to prevent unauthorized information changes (creation, alternation, and deletion). (INTEG2)	3.68 (1.29)	58 (33%)	57 (32%)	26 (15%)	19 (11%)	17 (10%)
<i>Availability</i>						
Authorized users in my organization have access to the company's information when needed and at anyplace. (AVAIL1)	3.87 (1.09)	54 (31%)	78 (44%)	21 (12%)	16 (9%)	8 (5%)
There are well established information access control procedures in my organization, to ensure that only authenticated users with right privileges can access such resource. (AVAIL2)	3.95 (1.19)	72 (41%)	59 (33%)	24 (14%)	9 (5%)	13 (7%)

Note. The variable information in parentheses, e.g., (CONF1) is used to identify items in the following tables. 1= Strongly Disagree, 2=Disagree, 3=No Opinion, 4=Agree, 5=Strongly Agree.

The inter-item correlation matrix and item-total reliability statistics are for the Information Security Management items are shown in Table 7. As shown, the highest inter-item correlation was for the first integrity item (INTEG1) with the second availability item (AVAIL2), with a correlation of .486. The lowest inter item correlation was for the two confidentiality items, with a correlation of .100.

Table 7

Inter-Item Correlation Matrix for Information Security Management

	My org enforces technical control to protect InfoSec. (CONFID1)	My org has well executed InfoSec practices to protect data (CONFID2)	My org updates information resources for integrity (INTEG1)	There is change mgmt. control in my org for integrity (INTEG2)	Only authorized users have access to information (AVAIL1)	There is an established control in my org (AVAIL2)
CONFID1	1.000	.100	.442	.415	.323	.395
CONFID2	.100	1.000	.442	.418	.339	.326
INTEG1	.442	.442	1.000	.450	.276	.486
INTEG2	.415	.418	.450	1.000	.313	.374
AVAIL1	.323	.339	.276	.313	1.000	.457
AVAIL2	.395	.326	.486	.374	.457	1.000

Note. CONF=Confidentiality, Integ=Integrity, Avail=Availability, Org=Organization

The Cronbach's alpha for the item-total reliability statistics scale (comprised of the six items) was .781. This indicates acceptable internal consistency reliability for the ISM section score. Each of the items showed adequate reliability statistics with the total score.

The item-total reliability statistics are shown in Table 8. The Cronbach's alpha for the scale (comprised of the six items) was .781. This indicates acceptable internal consistency reliability for the ISM section score. Each of the items showed adequate reliability statistics with the total score.

Table 8

Item-Total Reliability Statistics for Information Security Management

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
CONFID1	19.11	17.778	.474	.340	.760
CONFID2	19.07	17.591	.461	.335	.763
INTEG1	19.35	15.922	.608	.422	.727
INTEG2	19.34	15.725	.564	.344	.739
AVAIL1	19.15	17.649	.477	.282	.760
AVAIL2	19.07	16.189	.584	.373	.733

Note. CONF=Confidentiality, Integ=Integrity, Avail=Availability. Cronbach's Alpha (6 items) = .781

Table 9 describes the means for the three sub-domains (Confidentiality, Integrity, and Availability) as well as the total ISM mean for the six items in the section. The sub-construct with the highest mean was confidentiality (M = 3.93, SD = 0.81), and integrity had the lowest mean (M = 3.67, SD = 1.06). The total mean for ISM was 3.84 (SD = .80).

Table 9

The Means for the Three sub-Domains (Confidentiality, Integrity, Availability)

	ISM	Confidentiality	Integrity	Availability
N	177	177	177	177
Mean	3.84	3.93	3.67	3.91
Std. Deviation	.80	.81	1.06	.97
Minimum	1.67	1.50	1.00	1.50
Maximum	5.00	5.00	5.00	5.00
Skewness (Std. Error = .183)	-.469	-.549	-.543	-.904
Kurtosis (Std. Error = .363)	-.473	-.314	-.675	-.008

Note. ISM – Information Security Management

Each of the variables showed some negative skewness (particularly availability). Negative kurtosis was also evident (indicating flatness to the distributions). While there were some low scores outside the interquartile ranges on the confidentiality and availability domains (see Figure 4), there were no outliers for any of the scores with Z scores greater than ± 3.29 . The distributions are depicted using boxplots in Figure 4.

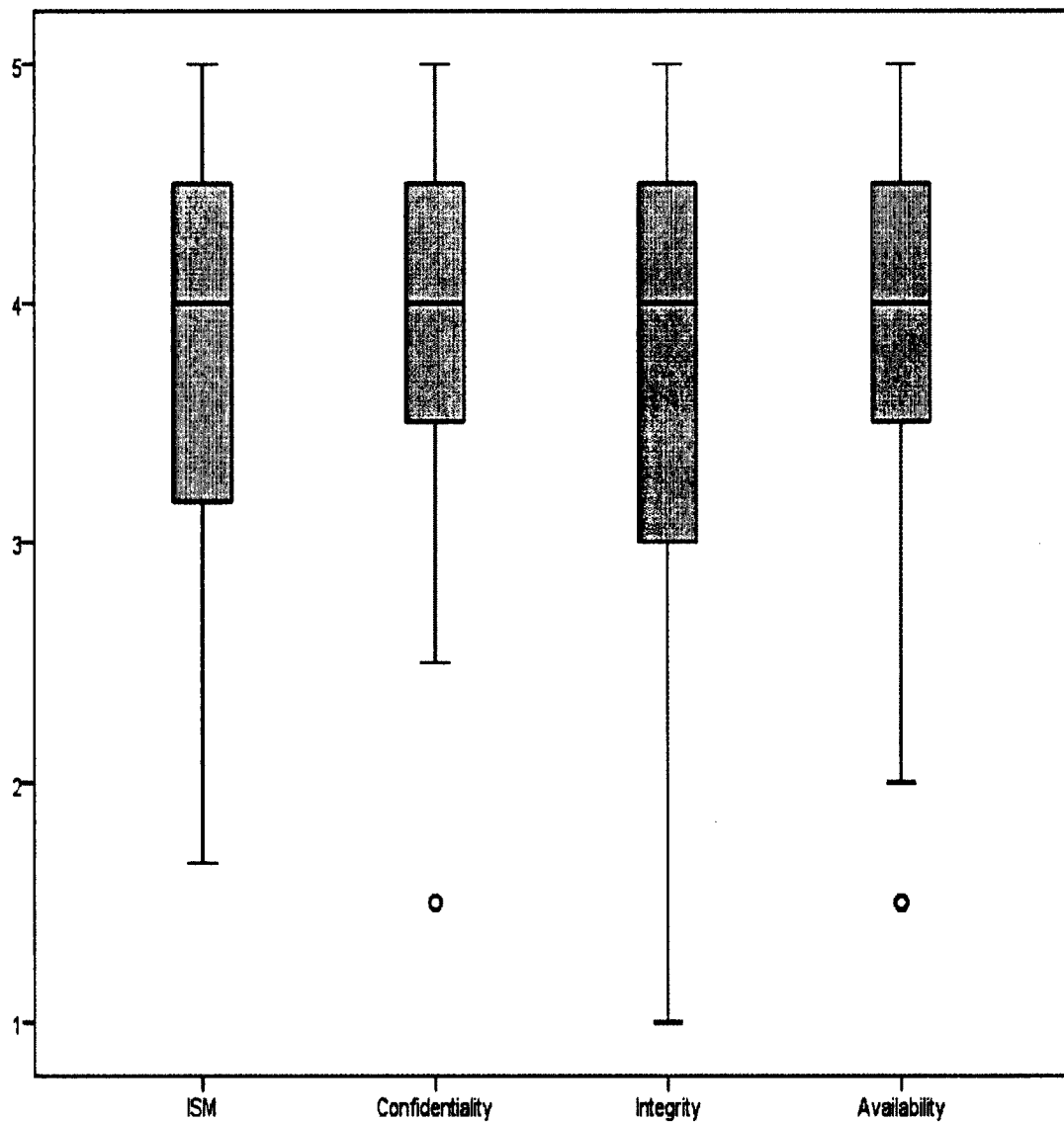


Figure 4. Boxplots of Information Security Management (ISM) and sub-dimensions

Information security policy – independent variable. The independent variable information security policy was comprised of two dimensions: User awareness and training, and behavior intention. The distribution of responses and means for the items are shown in Table 10. The highest mean was in the behavior intention domain, “I intend to assist others in complying with information security policies” ($M = 4.02$). The lowest mean in the behavior intention domain was for the item, “I intend to recommend that others comply with information security policies” ($M = 3.89$). The highest mean in the user awareness and training domain was “My organization has specific guidelines that govern what employees are allowed to do with their computers” ($M = 3.94$). The lowest mean in this domain was “My organization provides training to help employees improve their awareness of computer and information security issues” ($M = 3.31$).

Table 10

Item Responses for Information Security Policy

Item	Mean (SD)	Distribution of Responses				
		5	4	3	2	1
<i>User Awareness and Training</i>						
My org provides training to help improve InfoSec. awareness. (AWARE1)	3.31 (1.31)	35 (20%)	57 (32%)	36 (20%)	25 (14%)	24 (14%)
My org has guidelines that govern what employees are allowed to do with their computers. (AWARE2)	3.94 (1.12)	61 (34%)	76 (43%)	20 (11%)	8 (5%)	12 (7%)
My org has made training materials available to all (AWARE3)	3.69 (1.25)	51 (29%)	70 (40%)	25 (14%)	13 (7%)	18 (10%)
The InfoSec. policy in my org is visibly written. (AWARE4)	3.32 (1.29)	37 (21%)	53 (30%)	38 (21%)	28 (16%)	21 (12%)
<i>Behavior Intention</i>						
I intend to ignore InfoSec. Policies because it is an imposition. (INTENT1)	3.90 (1.11)	55 (31%)	83 (47%)	16 (9%)	12 (7%)	11 (6%)
I intend to play a role in the protection of InfoSec. in my org (INTENT2)	3.98 (1.11)	65 (37%)	76 (43%)	14 (8%)	12 (7%)	10 (6%)
I intend to recommend that others comply with InfoSec. policies. (INTENT3)	3.89 (1.11)	54 (31%)	84 (47%)	16 (9%)	12 (7%)	11 (6%)
I intend to assist others in complying with InfoSec. policies. (INTENT4)	4.02 (1.03)	65 (37%)	74 (42%)	22 (12%)	9 (5%)	7 (4%)

Note. The variable information in parentheses, e.g., (AWARE1) is used to identify items in the following tables. 1=Strongly Disagree, 2= Disagree, 3= No Opinion, 4=Agree, 5= Strongly Agree. Orgn=organization, InfoSec=Information Security.

The highest mean was in the behavior intention domain, “I intend to assist others in complying with information security policies” (M = 4.02). The lowest mean in the

behavior intention domain was for the item, “I intend to recommend that others comply with information security policies” ($M = 3.89$). The highest mean in the user awareness and training domain was “My organization has specific guidelines that govern what employees are allowed to do with their computers” ($M = 3.94$). The lowest mean in this domain was “My organization provides training to help employees improve their awareness of computer and information security issues” ($M = 3.31$).

The inter-item correlation matrix is shown in Appendix I. It can be seen that the item “I intend to ignore or circumvent security policies and controls because it is an imposition.” (INTENT1) was negatively related to item “There are specific awareness guidelines that govern employees’ computer usage” (AWARE2). However, both of these items were positively related to the other items within the section. Thus, reverse-coding either one of these items would lead to several negative correlations with the other items in the section. As such, they were retained in their original format.

The item-total statistics for the eight Security policy items and descriptive statistics for security policy sub-dimensions are shown in Tables 11 and 12 respectively. Each of the items shared adequate variance with the rest of the scale. The lowest correct item-total correlation was for item INTENT1 ($r = .318$). The Cronbach’s alpha value for the total section was .745, for user awareness the alpha was .665, and the behavior intention alpha was .608. This indicates adequate internal consistency for the section total, and questionable internal consistency for the two sub-domain scores.

Table 11

Item Total Statistics for Security Policy

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
AWARE1	26.75	23.120	.523	.315	.701
AWARE2	26.12	25.253	.437	.344	.719
AWARE3	26.36	24.459	.438	.296	.719
AWARE4	26.73	23.969	.456	.271	.716
INTENT1	26.16	26.554	.318	.237	.740
INTENT2	26.07	25.330	.434	.320	.720
INTENT3	26.16	25.433	.427	.211	.721
INTENT4	26.03	25.317	.488	.300	.712

Note. Cronbach's alphas: Security Policy (8 items) = .745, User awareness (4 items) = .665, Behavior intention (4 items) = .608.

In terms of the descriptive statistics for the security policy domain and the two sub-domains, the mean for security policy was 3.76 (SD = .70) with a range of scores from 1.50 to 5.00 out of a possible total of 5. As shown in Table 12, the mean for user awareness and training was 3.57 (SD = .78) and the mean for behavior intention was slightly higher at 3.95 (SD = .74).

Table 12

Descriptive Statistics for Security Policy and sub-Dimensions

	Security Policy	User Awareness and Training	Behavior Intention
N	177	177	177
Mean	3.76	3.57	3.95
Std. Deviation	.70	.88	.74
Minimum	1.50	1.00	1.25
Maximum	5.00	5.00	5.00
Skewness (Std. Error = .183)	-.565	-.404	-1.003
Kurtosis (Std. Error = .363)	.614	-.316	.982

The Boxplots showing the distribution of scores are depicted in Figure 5. The mean for security policy was 3.76 (SD = .70) with a range of scores from 1.50 to 5.00 out of a possible total of 5. The mean for user awareness and training was 3.57 (SD = .78) and the mean for behavior intention was slightly higher at 3.95 (SD = .74). All the variables were slightly negatively skewed (as also seen by the outlier points on the boxplots). For security policy and user awareness, there were no outliers with Z scores in excess of ± 3.29 . However, for behavior intention, there was one negative outlier with a Z score of -3.66 (Behavior intention score = 1.25). This case was removed during the analyses of the research questions.

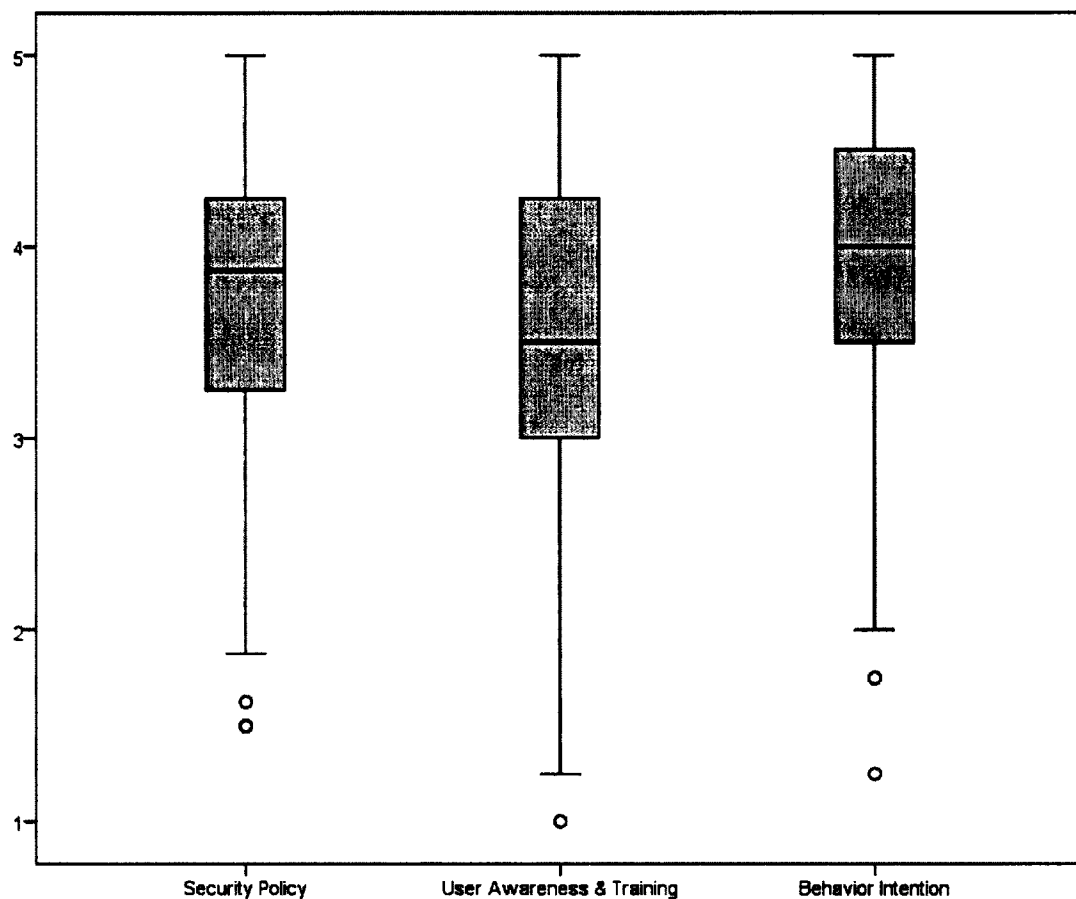


Figure 5. Boxplots for Security Policy and sub-dimensions

Organizational culture – independent variable. The organizational culture variable was comprised of the sub-dimensions of leadership support and normative beliefs. Table 13 shows the distribution of responding to the items in these dimensions.

Table 13

Item Responses for Organizational Culture

Item	Mean (SD)	Distribution of Responses				
		5	4	3	2	1
<i>Leadership Support</i>						
Top management style in my organization is characterized by conformity to good security practices. (LEAD1)	3.84 (1.12)	60 (34%)	61 (34%)	28 (16%)	23 (13%)	5 (3%)
Top management considers information security an important organizational significance. (LEAD2)	3.64 (1.18)	45 (25%)	68 (38%)	32 (18%)	19 (11%)	13 (7%)
Top management in my organization view information security as part of our overall strategy. (LEAD3)	3.58 (1.24)	47 (27%)	62 (35%)	29 (16%)	25 (14%)	14 (8%)
Top management pays ample attention to an information security strategy in order to protect information. (LEAD4)	3.82 (1.07)	47 (27%)	80 (45%)	32 (18%)	7 (4%)	11 (6%)
<i>Normative Beliefs</i>						
I comply with information security because it is a key norm shared by organizational members. (NORM1)	3.74 (1.12)	47 (27%)	75 (42%)	26 (15%)	20 (11%)	9 (5%)
I comply with information security policies because my supervisor wants me to. (NORM2)	3.60 (1.29)	52 (29%)	58 (33%)	27 (15%)	24 (14%)	16 (9%)
I comply with information security policies because my peers also do the same. (NORM3)	3.66 (1.20)	47 (27%)	68 (38%)	30 (17%)	18 (10%)	14 (8%)
I comply with information security policies due to top management in my organization. (NORM4)	3.59 (1.26)	47 (27%)	66 (37%)	24 (14%)	24 (14%)	16 (9%)

Note: 1= Strongly Disagree, 2= Disagree, 3= No Opinion, 4= Agree, 5= Strongly Agree.

All the means fell within a fairly narrow range. The low mean of 3.58 was for “Top management in my organization view information security as part of our overall strategy” and the highest mean of 3.84 was for “Top management style in my organization is characterized by conformity to good security practices.”

The reliability statistics and the means and the distributions for the organizational culture section and sub-dimensions are shown in Tables 14. Each item was moderately to highly correlated with the total scale. The Cronbach’s alpha for the organizational culture section was .791 indicating acceptable to good internal consistency. The internal consistency of the leadership support sub-dimension was poor/questionable (alpha = .585), and the internal consistency of normative beliefs was slightly higher, and in the acceptable range (alpha = .679).

Table 14

Item-Total Statistics for Organizational Culture Items

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
LEAD1	25.62	28.771	.551	.400	.760
LEAD2	25.82	29.524	.444	.272	.776
LEAD3	25.88	28.666	.484	.316	.770
LEAD4	25.64	30.903	.388	.190	.784
NORM1	25.72	28.942	.532	.317	.763
NORM2	25.86	27.452	.560	.360	.757
NORM3	25.80	29.489	.437	.219	.777
NORM4	25.87	27.352	.582	.365	.753

Note. Cronbach’s alphas: Organizational culture (8 items) = .791, Leadership support (4 items) = .585, Normative beliefs (4 items) = .679.

Regarding the means and the distributions for the organizational culture section and sub-dimensions (Table 15), the leadership support was 3.72 and the mean for

normative beliefs was 3.65. This equated to an overall section mean of 3.68. Each of the variables was slightly negatively skewed.

Table 15

Descriptive Statistics for Organizational Culture and sub-Dimensions

	Organizational Culture	Leadership Support	Normative Beliefs
N	177	177	177
Mean	3.68	3.72	3.65
Std. Deviation	.76	.77	.87
Minimum	1.75	1.50	1.00
Maximum	5.00	5.00	5.00
Skewness (Std. Error = .183)	-.101	-.229	-.397
Kurtosis (Std. Error = .363)	-.878	-.752	-.412

The inter-item correlation matrix for the items in this section (see Appendix J) indicate that the correlations were in the small to moderate range, and there were no negative correlations suggesting the need for reverse coding.

The boxplots for Organizational Culture and sub-dimensions is shown in Figure 6. The mean for There were no outliers with Z scores in excess of ± 3.29 on any of the scores. The organizational culture and leadership support were not skewed, while normative beliefs showed moderate negative skewness.

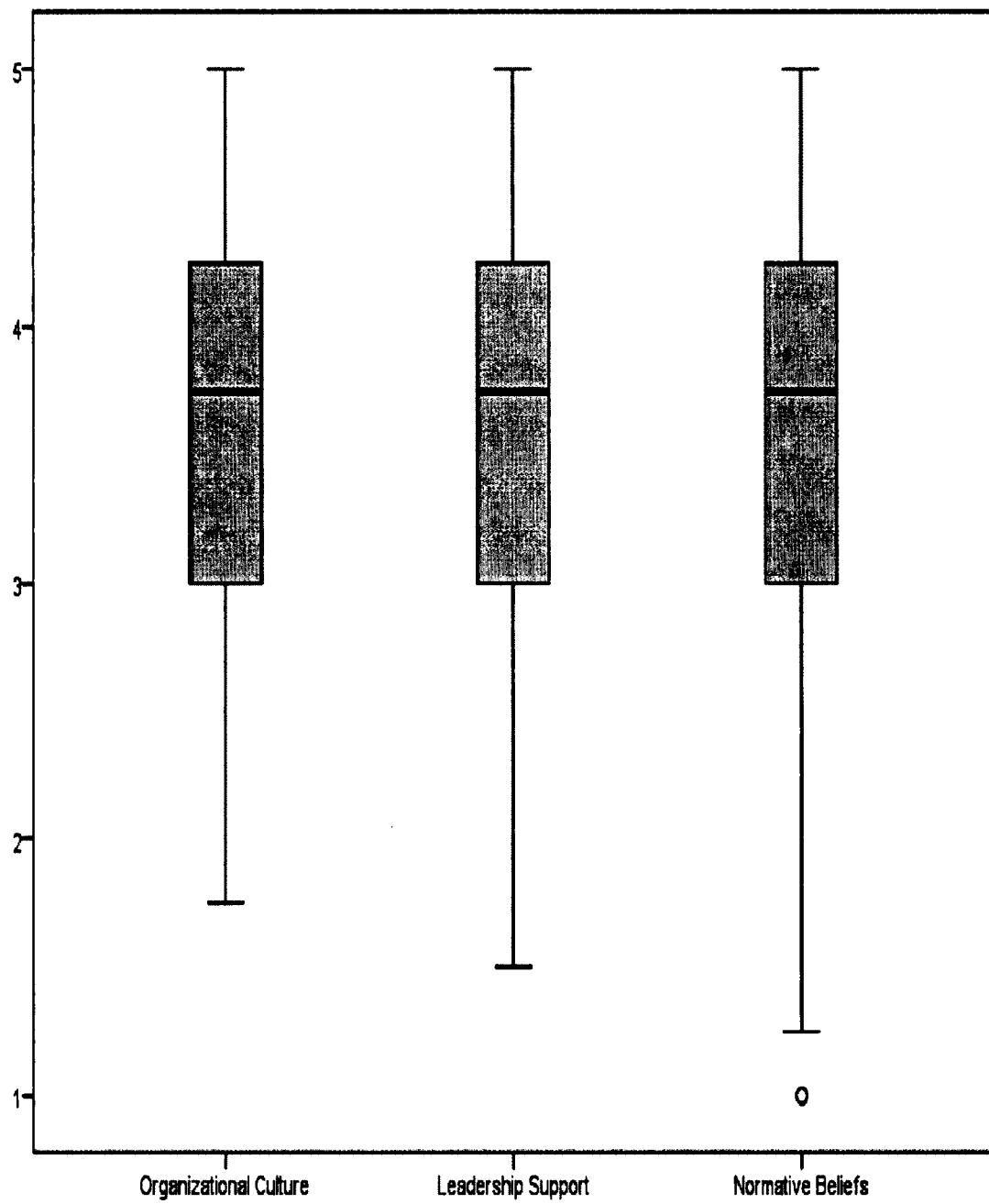


Figure 6. Boxplots for Organizational Culture and sub-dimensions

Human behavior actions – independent variable. The human behavior actions (see Table 16) variable was comprised of two sub-dimensions: Compliance behavior and deterrent countermeasures.

Table 16

Item Responses for Human Behavior Actions

Item	Mean (SD)	5	4	3	2	1
<i>Compliance behavior</i>						
I always lock my work computer screen or a screen saver whenever I leave my desk/office. (COMPLY1)	3.31 (1.35)	40 (23%)	53 (30%)	29 (16%)	32 (18%)	23 (13%)
My organization monitors any modification of computerized data by employees. (COMPLY2)	3.51 (1.36)	55 (31%)	48 (27%)	26 (15%)	29 (16%)	19 (11%)
Periodic audits are conducted in my org for unauthorized software usage. (COMPLY3)	3.46 (1.39)	54 (31%)	47 (27%)	25 (14%)	29 (16%)	22 (12%)
My org. monitors employees' use of Internet and other social-media sites. (COMPLY4)	3.75 (1.10)	46 (26%)	75 (42%)	32 (18%)	14 (8%)	10 (6%)
<i>Deterrent Countermeasure</i>						
I could be in trouble if I download anything from the web without scanning. (DETER1)	3.68 (1.30)	61 (34%)	53 (30%)	23 (13%)	26 (15%)	14 (8%)
I follow the InfoSec. policies because of future consequences. (DETER2)	3.77 (1.20)	61 (34%)	55 (31%)	32 (18%)	18 (10%)	11 (6%)
I could be suspended or dismissed if I breach data in my org (DETER3)	3.67 (1.29)	62 (35%)	46 (26%)	31 (18%)	25 (14%)	13 (7%)
If I do not follow my organization's InfoSec. polices, I will be severely penalized. (DETER4)	3.79 (1.17)	53 (30%)	72 (41%)	26 (15%)	13 (7%)	13 (7%)

Note. The variable information in parentheses, e.g., (COMPLY1) is used to identify items in the tables. 1= Strongly Disagree, 2.=Disagree, 3=No Opinion, 4=Agree, 5= Strongly Agree.

As shown in Table 16, the highest means were in the deterrent countermeasure domain, and the item with the highest mean was “If I do not follow my organization’s information security policies, I will be severely penalized (M = 3.79). The lowest mean was for the item in the compliance behavior section: “I always comply and lock my work computer screen or a screen saver whenever I leave my desk/office” (M = 3.31).

The item total statistics are shown in Table 17. The Cronbach’s alpha for the section was .648, indicating fair internal consistency for the section, and this level of internal consistency is deemed acceptable for research purposes. The alpha for compliance behavior was .462 and for normative beliefs the alpha was .544. Thus, the internal consistency reliabilities of the sub-dimensions were poor. The means were created by averaging across the constituent items identified in the section.

Table 17

Item-Total Reliability Statistics for Human Behavior Actions

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
COMPLY1	25.64	23.719	.338	.149	.618
COMPLY2	25.44	24.668	.255	.106	.641
COMPLY3	25.49	23.547	.332	.139	.620
COMPLY4	25.20	24.754	.366	.181	.612
DETER1	25.27	24.244	.317	.152	.623
DETER2	25.18	23.819	.401	.265	.602
DETER3	25.28	22.454	.482	.320	.579
DETER4	25.17	25.619	.253	.102	.638

Note. Cronbach’s alphas: Human Behavior Actions (8 items) = .648, Compliance Behavior (4 items) = .462, Deterrent Countermeasures (4 items) = .544.

The descriptive statistics for the means are shown in Table 18. The mean for compliance behavior was 3.51 and the mean for deterrent countermeasures was 3.73. The overall section mean was 3.62. None of the variables were excessively skewed, although they all showed negative kurtosis (indicating flatness to the distributions).

Table 18

Descriptive Statistics for Human Behavior Actions and sub-Dimensions

	Human Behavior Actions	Compliance Behavior	Deterrent Countermeasures
N	177	177	177
Mean	3.62	3.51	3.73
Std. Deviation	.68	.81	.81
Minimum	1.75	1.50	1.50
Maximum	5.00	5.00	5.00
Skewness (Std. Error = .183)	.141	.016	-.349
Kurtosis (Std. Error = .363)	-.392	-.605	-.631

The inter-item correlations for human behavior action are shown in appendix K. Most of the correlations (as shown in appendix K) were in the small range; however, there were no negative correlations that would suggest reverse coding was required.

The boxplots showing the distributions of the variables are in Figure 7. There were no outliers with Z scores in excess of $Z \pm 3.29$.

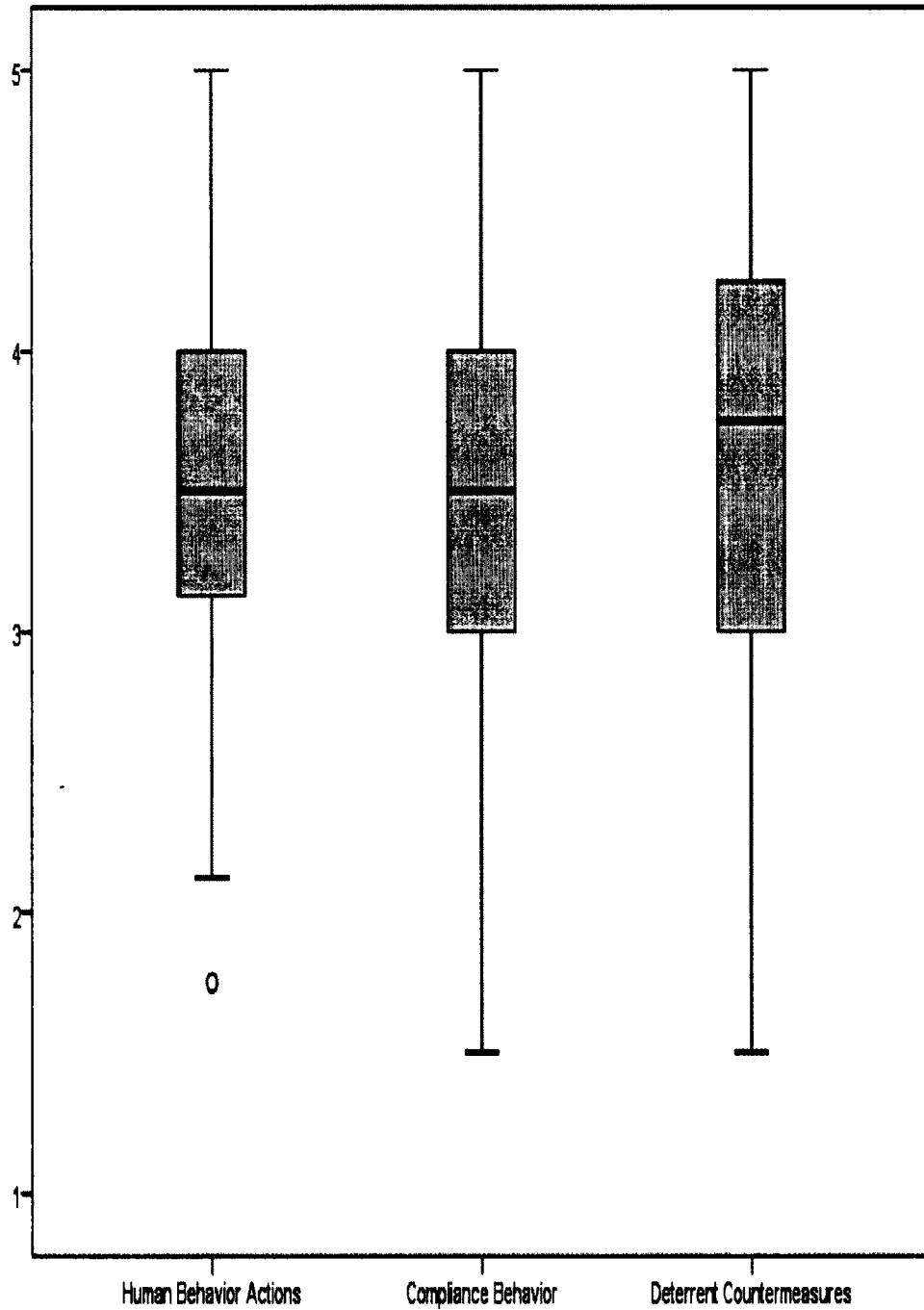


Figure 7. Boxplots for Human Behavior Actions and sub-dimensions

Additional analyses. Multivariate outliers data screening were examined by calculating Mahalanobis distance values. With 2 variables, the Chi-square critical value at $p < .001$ for a multivariate outlier is 13.816. For 3 variables, the critical value is 16.266, and for 4 variables, the critical value is 18.467. Examination for bivariate outliers between the dependent variable of information security management and each of the IVs separately revealed one outlier for ISM and security policy ($D^2 = 16.63$) with a Mahalanobis distance value greater than the critical value of 13.816. There were no multivariate outliers exceeding the critical values for the pairings of information security management and organizational culture, or for information security management and human behavior actions. Screening for information security management and the and three IVs together revealed two cases with Mahalanobis distances greater than the critical value of the chi-square distribution with four degrees of freedom (18.467). One of these was the bivariate outlier between information security management and security policy that had been previously identified. Given that there were only three outliers in total identified through the univariate and multivariate screening procedures, these responses were simply excluded during analyses of the research questions to ensure a consistent base of respondents for each question.

As shown in the previous section describing the variable scores, all the individual variables were relatively normally distributed. To provide a further check of the assumptions of regression in each analysis, the residual histograms and scatterplots were examined to provide a test of the assumptions of normality, linearity and homoscedasticity between the predicted DV scores and errors of prediction. There were no instances of violation of these assumptions of linear regression.

A number of regression procedures were used to clarify the relationships between the study variables. Bivariate regression was used for each research question, to determine to what extent there was a relationship between the DV and each of the IVs (i.e., what percentage of variance was explained). Pearson product-moment correlation coefficients were computed between the dependent variable of Information Security Management and the independent variables of security policy, organizational culture, and human behavior actions.

Research question RQ1. The following is a restatement of Research Question RQ1 and its associated null and alternative hypotheses.

RQ1. To what extent (if any) is there a relationship between security policy, as measured by user awareness and behavior intention, and Information Security Management, as measured by confidentiality, integrity, and availability?

H₁₀: There is no statistically significant relationship between organizational culture as measured by leadership support and normative beliefs, and Information Security Management, as measured by confidentiality, integrity, and availability.

H_{1a}: There is a statistically significant relationship between organizational culture as measured by leadership support and normative beliefs, and Information Security Management, as measured by confidentiality, integrity, and availability.

Correlation and bivariate linear regression were used to investigate the relationship between security policy and Information Security Management (ISM). The scatterplot of the relationship is shown in Figure 8.

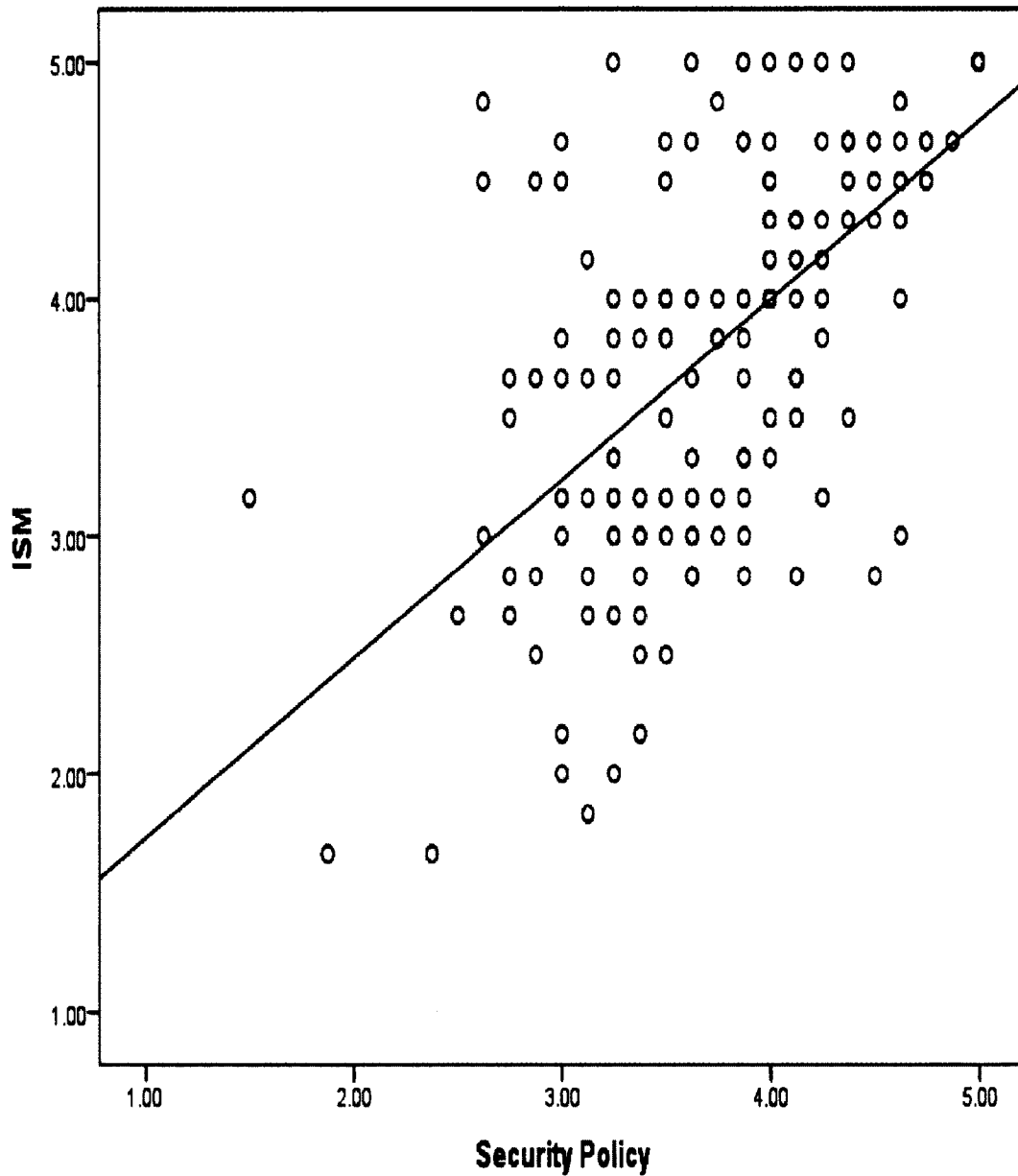


Figure 8. Scatterplot between ISM and Security Policy, with linear regression line.
 $R = .612$ ($p < .001$), $Y = .978 + .754x$, $R^2 = .375$, $\text{Adj. } R^2 = .372$. $N = 174$.

There was a large, positive correlation between the two variables, $r = .612$ ($p < .001$). The linear regression indicated that 37.2% of the adjusted variance in ISM was accounted for by the security policy scores.

Correlations were also computed between the sub-domains of each section. As shown in Table 19, positive, statistically significant correlations were observed between each sub-domain of ISM (confidentiality, integrity, and availability) and the two subdomains of security policy (user awareness and training, behavior intention).

Table 19

Correlations Between sub-Dimensions of ISM and of Security Policy

	Confidentiality	Integrity	Availability	User Awareness & Training	Behavior Intention
Confidentiality	1	.688**	.547**	.520**	.455**
Integrity	.688**	1	.497**	.455**	.450**
Availability	.547**	.497**	1	.416**	.354**
User Awareness & Training	.520**	.455**	.416**	1	.445**
Behavior Intention	.455**	.450**	.354**	.445**	1

Note. ISM = Information Security Management. Confidentiality, Integrity and Availability are sub-dimensions of ISM. User Awareness & training, and Behavior Intention are sub-dimensions of Security Policy. $N = 174$.

*. Correlation is significant at the 0.05 level (2-tailed). **. Correlation is significant at the 0.01 level (2-tailed).

For each sub-domain of ISM, the correlations were slightly larger with the user awareness and training scores than with the behavior intention scores. However, the correlations were in the medium to large range for both sets of relationships.

Multivariate multiple regression was used to investigate the combined relationship of the sub-dimensions. The multivariate effects from this analysis are shown in Table 20. There were significant multivariate effects of both user awareness and training and of behavior intention on the three sub-domains of ISM (p values $< .001$). The partial η^2 for

user awareness was 18.4% and behavior intention accounted for 11.8% of the variance in ISM sub-domain scores.

Table 20

Multivariate Effects of ISM sub-Domain on Security Policy sub-Domain Scores.

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	.117	7.469 ^b	3.000	169.000	.000	.117
User Awareness	Pillai's Trace	.184	12.661 ^b	3.000	169.000	.000	.184
Behavior Intention	Pillai's Trace	.118	7.569 ^b	3.000	169.000	.000	.118

a. Design: Intercept + Awareness + Behave.Intention

b. Exact statistic

The tests of between-subjects effects are shown in Table 21. Each of the sub-domains of confidentiality, integrity, and availability was significantly predicted from the two sub-domains of security policy ($p < .001$ for each analysis). All three of the ISM sub-domain scores were significantly predicted from user awareness ($p < .001$ for each analysis) and from behavior intention ($p < .01$ for each analysis). Thus, when all the variables were considered simultaneously, user awareness and training and behavior intention were both significantly predictive of each of the ISM sub-domains of confidentiality, integrity, and availability.

Table 21

Subjects Effects of ISM sub-Domain on Security Policy sub-Domain Scores.

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Confidentiality	38.532 ^a	2	19.266	42.691	.000	.333
	Integrity	54.857 ^b	2	27.428	33.818	.000	.283
	Availability	34.426 ^c	2	17.213	22.565	.000	.209
Intercept	Confidentiality	6.773	1	6.773	15.009	.000	.081
	Integrity	.585	1	.585	.722	.397	.004
	Availability	8.637	1	8.637	11.323	.001	.062
User Awareness	Confidentiality	14.534	1	14.534	32.206	.000	.158
	Integrity	15.676	1	15.676	19.328	.000	.102
	Availability	13.732	1	13.732	18.001	.000	.095
Behavior Intention	Confidentiality	7.235	1	7.235	16.033	.000	.086
	Integrity	14.768	1	14.768	18.208	.000	.096
	Availability	5.877	1	5.877	7.704	.006	.043
Error	Confidentiality	77.170	171	.451			
	Integrity	138.691	171	.811			
	Availability	130.444	171	.763			

a. R Squared = .333 (Adjusted R Squared = .325)

b. R Squared = .283 (Adjusted R Squared = .275)

c. R Squared = .209 (Adjusted R Squared = .200)

Research question RQ2. The following is a restatement of Research Question RQ2 and its associated null and alternative hypotheses.

RQ2: To what extent (if any) is there a relationship between organizational culture, as measured by leadership support and normative beliefs, and Information Security Management, as measured by confidentiality, integrity, and availability?

H₂₀: There is no statistically significant relationship between security policy as measured by user awareness and behavior intention, and Information

Security Management, as measured by confidentiality, integrity, and availability.

H2_a: There is a statistically significant relationship between security policy as measured by user awareness and behavior intention, and Information Security Management, as measured by confidentiality, integrity, and availability.

To address this question, correlation and regression procedures were used to investigate this research question. As shown in Figure 9, a very substantial, statistically significant, positive correlation was observed between Information Security Management and organizational culture, $r = .751$ ($p < .001$).

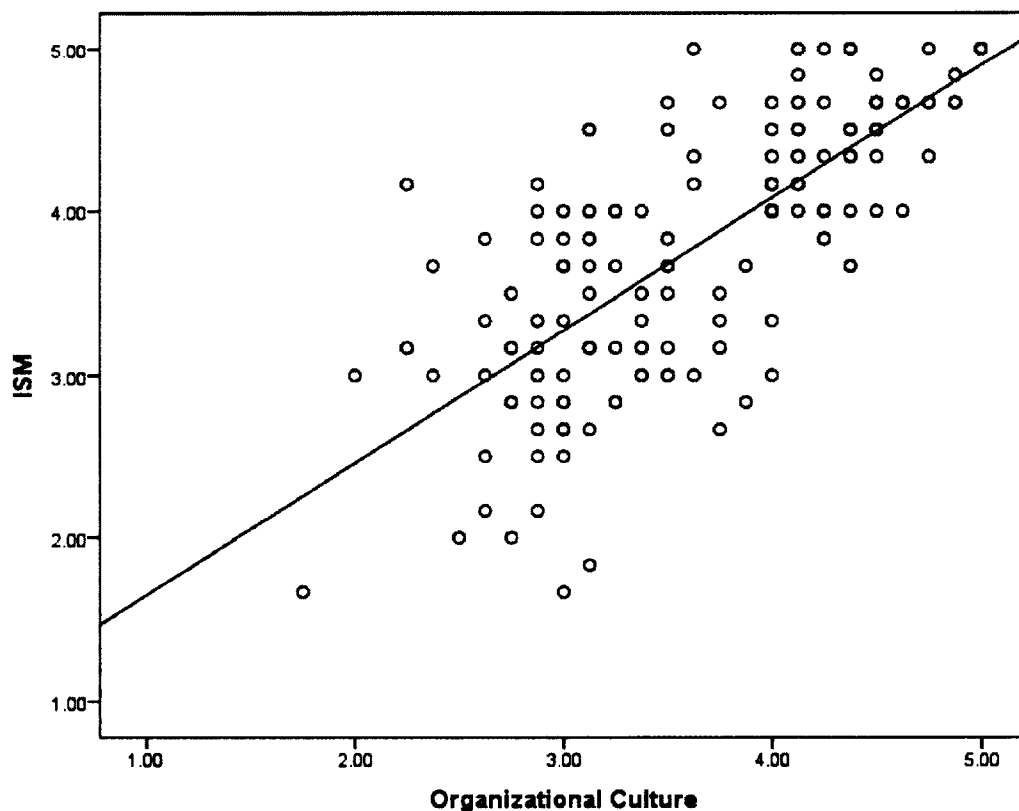


Figure 9. Scatterplot between ISM and Organizational Culture, with linear regression line. $R = .751$ ($p < .001$), $Y = .836 + .812x$, $R^2 = .565$, $Adj. R^2 = .562$.

The organizational culture scores accounted for 56.2% of the adjusted variance in Information Security Management scores. The correlations between the sub-domain scores of ISM and sub-dimensions of organizational culture are shown in Table 22. There were statistically significant and large correlations (i.e., above .6) between each of the sub-domains of ISM and leadership support. There were also large correlations (i.e., between .5-.6) between the sub-domains of Information Security Management and the normative beliefs scores.

Table 22

Correlations Between sub-Dimensions of ISM and Those of Security Culture

	Confidentiality	Integrity	Availability	Leadership Support	Normative Beliefs
Confidentiality	1	.688**	.547**	.670**	.518**
Integrity	.688**	1	.497**	.639**	.524**
Availability	.547**	.497**	1	.675**	.517**
Leadership Support	.670**	.639**	.675**	1	.701**
Normative Beliefs	.518**	.524**	.517**	.701**	1

Note. ISM = Information Security Management. Confidentiality, Integrity and Availability are sub-dimensions of ISM. Leadership support and Normative beliefs are sub-dimensions of Organizational culture.

*. Correlation is significant at the 0.05 level (2-tailed). **. Correlation is significant at the 0.01 level (2-tailed).

The results of the multivariate multiple regressions of the sub-domains of ISM on the sub-domains of organizational culture are presented in Tables 23 and 24. As revealed, there was a significant multivariate effect of leadership support ($p < .001$), yet not a significant effect of normative beliefs ($p = .243$) (Table 23). Leadership support accounted for 39.6% of the variance in the subdomains of ISM, whereas normative beliefs accounted for only 2.4% in the ISM subdomain scores.

Table 23

Multivariate Effects of ISM on organizational culture sub-domain scores.

Effect	Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	.152	10.123 ^b	3.000	169.000	.000
Leadership Support	Pillai's Trace	.396	36.949 ^b	3.000	169.000	.000
Normative Beliefs	Pillai's Trace	.024	1.404 ^b	3.000	169.000	.243

a. Design: Intercept +
Lead.Support + Norm.Belief

b. Exact statistic

Table 24 displays the between-subjects effects of multivariate multiple regression of ISM on security policy sub-domain. As seen (Table 24), each of the sub-domains of confidentiality, integrity, and availability was significantly predicted from the sub-domains of organizational culture (all p values $< .001$). However, this was primarily driven by the effects of leadership support. The leadership support sub-domain scores were significantly predictive of each sub-domain of ISM (all p values $< .001$). In contrast, there was no statistically significant relationship between normative beliefs and any of the ISM sub-domain scores, although the relationship between normative beliefs and integrity approached significance ($p = .070$).

Table 24

*Effects for Multivariate Multiple Regression of ISM on Security Policy sub-Domain**Scores.*

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Confidentiality	52.421 ^a	2	26.211	70.826	.000	.453
	Integrity	81.283 ^b	2	40.642	61.905	.000	.420
	Availability	75.705 ^c	2	37.852	72.593	.000	.459
Intercept	Confidentiality	9.539	1	9.539	25.776	.000	.131
	Integrity	.456	1	.456	.695	.406	.004
	Availability	2.763	1	2.763	5.299	.023	.030
Leadership Support	Confidentiality	21.337	1	21.337	57.657	.000	.252
	Integrity	28.178	1	28.178	42.921	.000	.201
	Availability	31.594	1	31.594	60.592	.000	.262
Normative Beliefs	Confidentiality	.545	1	.545	1.473	.227	.009
	Integrity	2.180	1	2.180	3.320	.070	.019
	Availability	.635	1	.635	1.217	.271	.007
Error	Confidentiality	63.282	171	.370			
	Integrity	112.264	171	.657			
	Availability	89.165	171	.521			

a. R Squared = .453 (Adjusted R Squared = .447)

b. R Squared = .420 (Adjusted R Squared = .413)

c. R Squared = .459 (Adjusted R Squared = .453)

Research question RQ3. The following is a restatement of Research Question RQ3 and its associated null and alternative hypotheses.

RQ3: To what extent (if any) is there a relationship between human behavior actions, as measured by compliance behavior and deterrent countermeasures, and Information Security Management, as measured by confidentiality, integrity, and availability?

H3₀: There is no statistically significant relationship between human behavior actions as measured by compliance behavior and deterrent countermeasures, and Information Security Management, as measured by confidentiality, integrity, and availability.

H3_a: There is a statistically significant relationship between human behavior actions as measured by compliance behavior and deterrent countermeasures, and Information Security Management, as measured by confidentiality, integrity, and availability.

Correlation and regression procedures were used to investigate this question. As shown in Figure 10, a large, positive relationship was observed between the variables of ISM and human behavior actions, $r = .646$ ($p < .001$). Linear regression indicated that human behavior action scores accounted for 41.4% of the adjusted variance in ISM scores. Furthermore, investigation of the relationships between the sub-domain scores was conducted using correlations. As shown in Table 25, there were moderate, statistically significant correlations ($\sim .4$) between the three sub-domains of ISM any compliance behavior scores. There were also moderate to large correlations between the domains of

ISM and the deterrent countermeasures scores, with correlations ranging from .456 for availability to .601 for integrity.

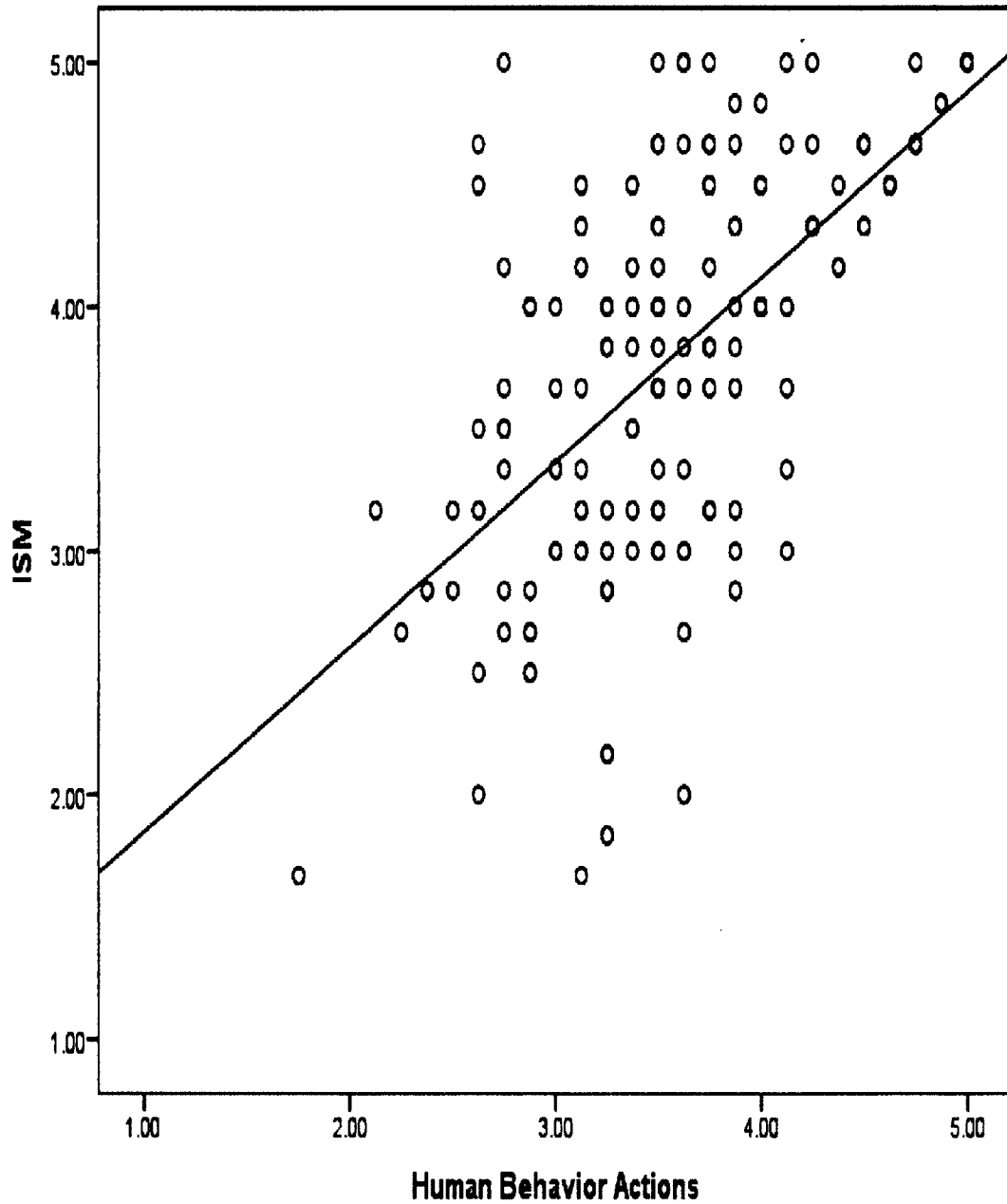


Figure 10. Scatterplot between ISM and Human Behavior Actions, with linear regression line. $R = .646$ ($p < .001$), $Y = 1.091 + .758x$, $R^2 = .417$, Adj. $R^2 = .414$.

Table 25

Correlations Between sub-Dimensions of ISM and Human Behavior Actions.

	Confidentiality	Integrity	Availability	Compliance Behavior	Deterrent Countermeasures
Confidentiality	1	.688**	.547**	.377**	.498**
Integrity	.688**	1	.497**	.446**	.601**
Availability	.547**	.497**	1	.402**	.456**
Compliance Behavior	.377**	.446**	.402**	1	.452**
Deterrent Countermeasures	.498**	.601**	.456**	.452**	1

Note. ISM = Information Security Management. Confidentiality, Integrity and Availability are sub-dimensions of ISM. Compliance behavior and deterrent countermeasures are sub-dimensions of Human Behavior Actions.

*. Correlation is significant at the 0.05 level (2-tailed). **. Correlation is significant at the 0.01 level (2-tailed).

Table 26 displays multivariate multiple regressions results scores for the examination of the relationships between the sub-domains.

Table 26

Multivariate Effects of ISM sub-Domain on Human Behavior Actions sub-Domain Scores.

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	.215	15.391 ^b	3.000	169.000	.000	.215
Compliance Behavior	Pillai's Trace	.092	5.690 ^b	3.000	169.000	.001	.092
Deterrent Countermeasures	Pillai's Trace	.278	21.690 ^b	3.000	169.000	.000	.278

a. Design: Intercept + Compliance.Beh + Deterrence

b. Exact statistic

There were significant multivariate effects for compliance behavior ($p = .001$) and for deterrent countermeasures ($p < .001$) on the three domains of Information Security

Management. Compliance behavior accounted for 9.2% of the variance, and deterrent countermeasures accounted for 27.8% of the variance in the combination of ISM sub-domain scores.

Investigation of between-subjects effects showed that each of the three ISM sub-domains was significantly predicted by the sub-domains of human behavior action (all p values $< .001$) (Table 27). Compliance behavior and deterrent countermeasures were both significantly predictive of all three sub-domains of confidentiality, integrity, and availability (all p values $< .01$), although the variance explained (by partial η^2 values) was greater for deterrent countermeasures than for compliance behavior.

Table 27

*Effects for Multivariate Multiple Regression of ISM on Human Behavior sub-Domain**Scores.*

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Confidentiality	32.090 ^a	2	16.045	32.815	.000	.277
	Integrity	77.253 ^b	2	38.627	56.797	.000	.399
	Availability	42.247 ^c	2	21.124	29.457	.000	.256
Intercept	Confidentiality	16.612	1	16.612	33.973	.000	.166
	Integrity	.227	1	.227	.333	.565	.002
	Availability	10.000	1	10.000	13.946	.000	.075
Compliance Behavior	Confidentiality	3.341	1	3.341	6.833	.010	.038
	Integrity	7.350	1	7.350	10.808	.001	.059
	Availability	7.910	1	7.910	11.031	.001	.061
Deterrent Countermeasures	Confidentiality	15.651	1	15.651	32.008	.000	.158
	Integrity	38.834	1	38.834	57.102	.000	.250
	Availability	15.642	1	15.642	21.814	.000	.113
Error	Confidentiality	83.612	171	.489			
	Integrity	116.294	171	.680			
	Availability	122.622	171	.717			

a. R Squared = .277 (Adjusted R Squared = .269)

b. R Squared = .399 (Adjusted R Squared = .392)

c. R Squared = .256 (Adjusted R Squared = .248)

Research question RQ4. The following is a restatement of Research Question RQ4 and its associated null and alternative hypotheses.

RQ4: To what extent (if any) do non-technical security management factors of security policy (measured by user awareness and behavior intention), organizational culture (measured by leadership support and normative beliefs), and human behavior actions (measured by compliance behavior and deterrent countermeasures) predict Information Security Management (measured by confidentiality, integrity, and availability)?

H₄₀: The non-technical security management factors of security policy, organizational culture, and human behavior actions, do not significantly predict Information Security Management, as measured by confidentiality, integrity, and availability.

H_{4a}: The non-technical security management factors of security policy, organizational culture, and human behavior actions, are significantly predictive of Information Security Management, as measured by confidentiality, integrity, and availability.

The correlations between the DV and the three IVs are shown in Table 28. As previously indicated, there were significant correlations between ISM and each of the three IVs. Furthermore, as indicated in the table, the three IVs were significantly correlated to one another. Thus, multiple regressions was employed to provide clarification regarding which IVs were most related to the ISM scores, when in the presence of the other variables.

Table 28

Correlation Coefficients Between ISM and the Three Independent Variables.

	ISM	Security Policy	Organizational Culture	Human Behavior Actions
ISM	1	.612**	.751**	.646**
Security Policy	.612**	1	.717**	.619**
Organizational Culture	.751**	.717**	1	.708**
Human Behavior Actions	.646**	.619**	.708**	1

Note. ISM = Information Security Management.

*. Correlation is significant at the 0.05 level (2-tailed). **. Correlation is significant at the 0.01 level (2-tailed).

The parameter coefficients from the multiple regression of ISM on the three IVs are shown in Appendix L. The regression equation was statistically significant, $F(3,170) = 83.524$, $p < .001$, and the three IVs together predicted 58.9% of the adjusted variance in ISM scores. Examination of the individual parameter statistics showed that both organizational culture ($p < .001$) and human behavior actions ($p = .004$) were significant, unique predictors of ISM. However, the coefficient for security policy was not significant ($p = .147$). Thus, when considering the prediction of ISM from the three IVs together, security policy did not contribute a statistically significant amount of prediction to ISM scores, over and above that already predicted by organizational culture and human behavior actions.

Multivariate multiple regression was also employed to examine which of the sub-dimensions of the IVs were most predictive of ISM sub-dimensions, when all the IVs were considered simultaneously. The multivariate effects from this analysis are shown in Table 29. The results showed that leadership support ($p < .001$) and deterrent countermeasures

($p = .001$) were statistically significant predictors of the three ISM sub-domain scores, while the other sub-dimensions of the IVs failed to reach statistical significance.

Table 29

Multivariate Effects of ISM and the Three IVs sub-Domain Scores.

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	.085	5.086 ^b	3.000	165.000	.002	.085
User Awareness	Pillai's Trace	.027	1.502 ^b	3.000	165.000	.216	.027
Behavior Intention	Pillai's Trace	.012	.682 ^b	3.000	165.000	.564	.012
Leadership Support	Pillai's Trace	.286	22.059 ^b	3.000	165.000	.000	.286
Normative Beliefs	Pillai's Trace	.003	.188 ^b	3.000	165.000	.904	.003
Compliance Behavior	Pillai's Trace	.017	.962 ^b	3.000	165.000	.412	.017
Deterrent Countermeasures	Pillai's Trace	.091	5.537 ^b	3.000	165.000	.001	.091

a. Design: Intercept + Awareness + Behave.Intention + Lead.Support + Norm.Belief + Compliance.Beh + Deterrence

b. Exact statistic

The between-subjects effects are presented in Table 30. The results showed that all three Information Security Management sub-domains were significantly predicted from the combination of IV sub-domains (all p values $< .001$). However, statistically significant effects were only present for some of the sub-domains of the independent variables.

Table 30

Subjects Effects Tests between ISM and the Three IVs sub-Domain Scores

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	Confidentiality	55.990 ^a	6	9.332	26.098	.000	.484
	Integrity	95.411 ^b	6	15.902	27.060	.000	.493
	Availability	76.700 ^c	6	12.783	24.213	.000	.465
Intercept	Confidentiality	2.297	1	2.297	6.425	.012	.037
	Integrity	1.106	1	1.106	1.882	.172	.011
	Availability	1.467	1	1.467	2.778	.097	.016
User Awareness	Confidentiality	1.428	1	1.428	3.992	.047	.023
	Integrity	.154	1	.154	.261	.610	.002
	Availability	.050	1	.050	.094	.759	.001
Behavior Intention	Confidentiality	.509	1	.509	1.425	.234	.008
	Integrity	.190	1	.190	.324	.570	.002
	Availability	.180	1	.180	.342	.560	.002
Leadership Support	Confidentiality	10.536	1	10.536	29.468	.000	.150
	Integrity	10.800	1	10.800	18.378	.000	.099
	Availability	22.952	1	22.952	43.472	.000	.207
Normative Beliefs	Confidentiality	.002	1	.002	.006	.937	.000
	Integrity	.008	1	.008	.013	.910	.000
	Availability	.274	1	.274	.519	.472	.003
Compliance Behavior	Confidentiality	.014	1	.014	.039	.843	.000
	Integrity	.965	1	.965	1.642	.202	.010
	Availability	.298	1	.298	.564	.454	.003
Deterrent Countermeasures	Confidentiality	.754	1	.754	2.110	.148	.012
	Integrity	9.541	1	9.541	16.236	.000	.089
	Availability	.516	1	.516	.977	.324	.006
Error	Confidentiality	59.713	167	.358			
	Integrity	98.137	167	.588			
	Availability	88.169	167	.528			

a. R Squared = .484 (Adjusted R Squared = .465)

b. R Squared = .493 (Adjusted R Squared = .475)

c. R Squared = .465 (Adjusted R Squared = .446)

Leadership support was a statistically significant predictor of all three sub-domains of ISM. User awareness was a statistically significant predictor of confidentiality ($p = .047$), and deterrent countermeasures was a statistically significant predictor of integrity ($p < .001$). The other sub-domain scores failed to reach statistical significant relationships with the ISM scores.

Evaluation of Findings

This research study was an examination of the relationship between non-technical components and management of information security in health informatics. In the last years, Information Security Practitioners have shifted their focus on people in the management and protection of information assets. This transference of strategy was based on the recognition by many in the information systems environment that comprehensive information security cannot be attained by just installing technical solutions like IDS, firewalls and implementing processes. Because it is the people in turn in these organizations who maintain the technology, maintain the day-to-day security processes, and influence the security strategy of their organizations (Beznosov & Beznosova 2007; Siponen et al., 2007). As a consequence it is imperative on all information security stakeholders to focus on non-technical factors in relation to how information security is managed.

Evaluation of findings for research question RQ 1: The first question of the study was aimed at examining the relationship Information Security Management, as measured by confidentiality, integrity, and availability and information security policy, as measured by user awareness and behavior intention. The study findings suggested that there is a relationship between security policy and the management of information security

indicating that security policy predicts the management of information security in organizations. Literature research found that when employees have increased awareness and adequate training, the more likely employees are to shape their behavior intention towards information security policy (Knapp et al., 2009; Siponen et al., 2010). As discussed by Siponen et al. (2010), organizations attain greater levels of security success when information security policy is the preliminary measure put in place in order to minimize the threat of objectionable use of any of the organizations' information resources.

Information security policy's impact on the management of information security was confirmed in the study as there was a positive correlation- $r=.612(p<.001)$ between the two variables. The mean for security policy was 3.76 (SD = .70) with a range of scores from 1.50 to 5.00 out of a possible total of 5. The mean for user awareness and training was 3.57 (SD = .78) and the mean for behavior intention was slightly higher at 3.95 (SD = .74). The results also showed that there was a significant zero-order correlation between the user awareness and behavior intention sub-domains of security policy, and the ISM sub-domains of confidentiality, integrity and availability. The finding is consistent with prior research (D'Arcy, Herath & Rao, 2009; Hovav & Galletta, 2008; Knapp et al., 2009; Siponen et al., 2010) that in an existing information security management paradigm, the role of security policy is crucial.

According to D'Arcy et al (2008), there is a direct and indirect influence of security policies on users' intentions with regard to information systems usage/abuse. They contended that, users are less likely to engage in information systems misuse when users are aware that security policies exist. Furthermore, as Knapp et al. (2009) explained,

not only does awareness prepare users to receive the rudimentary ideas of security through a proper training program, but it alerts people in organizations to the subjects of information security (Straub & Welke, 1998). In addition, Herath and Rao (2009) found that inherent incentive of employees' apparent effectiveness of their actions play a vital part in security policy compliance intentions of users.

The results in the study also confirmed the assertions by some of the researchers. In this study for example, while the highest mean in the user awareness and training domain was "My organization has specific guidelines that govern what employees are allowed to do with their computers" ($M = 3.94$), the highest mean in the behavior intention domain was "I intend to assist others in complying with information security policies" ($M = 4.02$).

Evaluation of findings for research question RQ 2: The next focus of the study was to examine the correlation between organizational culture, as measured by leadership support and normative beliefs, and Information Security Management, as measured by confidentiality, integrity, and availability. The organizational culture scores accounted for 56.2% of the adjusted variance in ISM scores. Study findings suggested that, consistency scores were statistically significant, $\beta = .76$, $p < .001$, and it was concluded that there was a positive relationship between the organizational and information security management. Based on the statistical tests, $r = .751$ ($p < .001$), there was a very considerable, statistically significant, positive correlation between Information security management and organizational culture. Also, there was a significant multivariate effect of leadership support ($p < .001$). Leadership support accounted for 39.6% of the variance in the subdomains of ISM, whereas normative beliefs accounted for only 2.4% in the ISM

subdomain scores. The level of consistency across with findings from research question 2 reveal that very considerable positive relationships exist between information security management and organizational culture.

The present study supports preceding researches (Chang & Ho, 2006; Dhillon & Torkzadeh, 2006; Kankanhalli et al., 2003; Knapp et al., 2009) in showing that leadership support and normative beliefs help in developing mindset and creating organizational culture that builds effective information security management strategy. These non-technical factors (subjective norms, leadership, belief, and human behavior of ISM activities) could be more effective means of achieving real information security management than just technical mechanisms such as firewall, anti-virus, etc. Knapp et al. (2009) surveyed a group of information security professionals with regard to the significance of top management support in forecasting policy implementation and security culture in organizations. The authors concluded that top management support is critical for executing security controls within organizations. Equally, Kankanhalli et al (2003) alleged that organizations that experience support from the top management often get the flexibility of huge allocation of resources to deploy advanced security software.

The study further supports the notion that security behaviors can be influenced by both inherent and extrinsic instigators. As Herath and Rao (2009) noted, apparent behavior of individuals, norms, attitudes and perceptions can be inferred from what the individuals say and do and core values. The present study also supports past research (Da Veiga & Eloff, 2009) in showing that information security employees' behaviors could be influenced by subjective norms and peer behaviors. In this study for example, the highest mean of 3.84 under the organizational culture variable was for "Top management style in

my organization is characterized by conformity to good security practices.” That encompasses the internal belief systems of each individual in the organization. Thus based on the research findings, information security management has a positive significant relationship with organizational culture.

Evaluation of findings for research question RQ 3. The third research question was designed with the aim at examining the relationship between human behavior actions, as measured by compliance behavior and deterrent countermeasures, and Information Security Management, as measured by confidentiality, integrity, and availability. Study findings suggest that in terms of human behavior actions, stakeholders are aware of the importance of compliance behavior and deterrence in regard to achieving effective information security management. Current research has shown that having adaptable human behavior actions not only increases the chances of successful information security management but also supports comprehensive information security strategy across the organization. As stated in some past studies (Chang & Lin, 2007; Da Veiga & Eloff, 2009; Siponen et al., 2010), human elements actions explain how different issues could lead to causes of security breaches and vulnerabilities in organizations.

Findings from this study support the premise that stakeholders in the healthcare industry understand the importance of security policy compliance and deterrence when issues of information security come into play. The overall relationship information security management and human behavior actions was a positive one, $r=.664$ ($p<.001$). The adjusted variance in ISM scores, human behavior action score amounted for 41.4%. Of the relationships between the sub-domain scores, there were significant multivariate effects of $p=.001$ for compliance behavior and $p<.001$ for deterrent countermeasures. The

mean for compliance behavior was 3.51. The findings is consistent with Herath and Rao (2009) assertion that core incentives of users' apparent effectiveness of their actions play an essential role in security policy compliance intentions; which greatly affect the overall management of information security in organizations.

Further, the present study supports past studies (D'Arcy et al., 2008; Kankanhalli et al., 2003; Straub, 1990) that certain countermeasures (deterrents) help deter information system misuse although some suggest deterrents have little, if any, effect on information security (Lee et al., 2004; Wiant, 2003). In this study, while the mean for deterrent countermeasures was 3.73, the item with the highest mean in this section was "If I do not follow my organization's information security policies, I will be penalized (M=3.79)."

Having statistically proven data further expands on this research in developing an understanding of the relationship between human behavior actions and information security management challenges that security experts have to face within their organizations. In all, the results indicated that the null hypotheses should be rejected and there is a positive relationship between ISM and human behavior actions.

Evaluation of findings for research question RQ 4: The focus of this final research question was examine the contribution of all three IVs of security policy (measured by user awareness and behavior intention), organizational culture (measured by leadership support and normative beliefs), and human behavior actions (measured by compliance behavior and deterrent countermeasures) to the prediction of Information Security Management (measured by confidentiality, integrity, and availability) using multiple regressions. According to Mirabella (2006), when conducting a Test or Correlation, a relationship is tested between two scale variables (one independent and one

dependent). The dependent variable (information security management), and the independent salient variables (organizational culture, security policy, and human behavior actions) were tested for correlation. Due to the presence of correlated predictors, multiple regressions were used to clarify which of the predictors were contributing unique variance, over and above that predicted by the other variables in the model. Multivariate multiple regression was used in the final research question to examine the relationship between all the sub-domains in the survey simultaneously.

The findings from research question four affirmed the main foundation of this study; non-technical factors have an impact on information security management. Statistical results in Table 30 indicated that three independent variables (IVs)-security policy, organizational culture, and human behavior action were significantly correlated to one another. The regression equation was less significant, $F(3,170) = 83.524$, $p < .001$, and the three IVs together predicted 58.9% of the adjusted variance in ISM scores. With regard to individual parameters, the coefficient for security policy was less significant ($p = .147$) to ISM than the parameter statistics of both human behavior actions ($p = .0004$) and organizational culture ($p < .001$). Of the relationships between the sub-domain scores, leadership support ($p < .001$) and deterrence countermeasures ($p < .001$) were statistically significant predictors of the three ISM sub-domain scores.

The study supports past researches (Chang & Lin, 2007; Da Veiga & Eloff, 2009; Dhillon & Torkzadeh, 2006; Kankanhalli et al., 2003; Knapp et al., 2009; Siponen et al., 2010) in showing that non-technical factors (in this case security policy, organizational culture, and human behavior actions) have been shown to influence not only the individual characteristics of information security, but also the overall strategy of information security

management in organizations. Additionally, the results from the study fully support the integrated framework of the study (GDT and TRA) in that when non-technical factors are better appreciated and incorporated into organizations' security strategy at the onset, they positively affect the management of information security in organizations.

Summary

The study involved examination of the impact of non-technical security management factors including organizational culture (leadership support and normative beliefs), security policy (user awareness and behavior intention), and human behavior actions (deterrent countermeasures and compliance behavior) on information security management in health informatics. One hundred seventy seven usable survey questionnaires were processed and the results were presented. Cronbach's alpha was used as a measure of reliability. The calculation of Cronbach's alpha coefficient indicates a satisfactory level of internal consistency of the study instrument. Pearson product-moment correlation coefficients were computed between the dependent variable of Information Security Management and the independent variables of security policy, organizational culture, and human behavior actions. Additionally, correlations were calculated between the sub-domain scores of each variable.

All four of the null hypotheses of this study were rejected. For research question RQ 1, the alternative hypothesis was accepted. There was a statistically significant, large and positive relationship between security policy as measured by user awareness and behavior intention, and Information Security Management, as measured by confidentiality, integrity, and availability. In regard to research question RQ 2, there was a large, positive, statistically significant relationship between organizational culture as measured by

leadership support and normative beliefs, and ISM, as measured by confidentiality, integrity, and availability: the alternative hypothesis was supported. The alternative hypothesis associated with RQ 3 was supported. There was a large, statistically significant relationship between human behavior actions as measured by compliance behavior and deterrent countermeasures, and ISM, as measured by confidentiality, integrity, and availability. Finally, the alternative hypothesis for RQ 4 was supported: the non-technical factors of security policy, organizational culture, and human behavior actions, were significantly predictive of ISM, as measured by confidentiality, integrity, and availability.

The evaluation of findings in this study included an interpretation of the results when compared to the conceptual framework. Furthermore, the findings are consistent with the previously recognized relationships in the context of non-technical security management factors and information security management in health informatics.

Chapter 5: Implications, Recommendations, and Conclusions

The problem addressed in this non-experimental quantitative study was the dearth of non-technical security measures in the formulation of information security management (ISM) by stakeholders in health informatics in Ghana. Whereas the adoption of Information and Communication Technology (ICT) by many governments has provided opportunities for operational efficiency and quality of services in both private and public sectors (Ciborra, 2005), there is concern drawn to the importance of the responsibility of protecting the information assets (Da Veiga & Eloff, 2009). While humans are the heart of information security for many years, yet often only the technical perspective (firewall, anti-virus, etc) of security management has been the main area of interest for many practitioners (Beznosov & Beznosova, 2007; Siponen et al., 2007). The present study integrated two prominent bodies of research, the theory of reasoned action (TRA) and general deterrence theory (GDT) to formulate the framework to examine the impact of non-technical elements and information security management. Non-technical measures play an important role in organizations' efforts to protect information assets against accidental mishaps, intentional theft and corruption of data, among others.

The purpose of this non-experimental quantitative study was to examine the impact of the non-technical security management factors including organizational culture (leadership support and normative beliefs), security policy (user awareness and behavior intention), and human behavior actions (deterrent countermeasures and compliance behavior) on information security management in health informatics. The quantitative design was chosen because it tolerates flexibility in eliminating potential issues with

extraneous variables that might need to be controlled, as well as evaluating correlation (Brady & Collier, 2004).

The sample population of this study encompassed healthcare professionals from the Korle-Bu Teaching Hospital (which include physician consultants, surgeons, anesthetists, pharmacists, nurses/midwives, pathologists, radiologists, and laboratory technologists), and technocrats from the Ministry of Health. Out of 200 surveys distributed, 177 responses were received. That was about 88% response rate. The study participants' responses were to answer the research questions. The research analyses involved descriptive statistics in order to characterize the demographic nature of the sample, and correlation analyses in hypothesis testing. The results of this study, like every research study, innately encountered some limitations due to many factors (Mathie & Carnozz, 2005). Thus the results from the present study need to be interpreted in the context of limitations.

The first limitation of the study was that the outcome of the study was generalized to the population of only two entities; the Korle-Bu Teaching Hospital (KBTH) and the Ministry of Health, from which the sample was obtained. A greater number of hospitals as well as institutions that may be directly or indirectly involved with ICT in Ghana were not included in the study due to the difficulty of getting permissions, and also due to cost. Thus the findings of this study may not be a true representative of the impact of non-technical factors on the management of information security in informatics.

Another limitation for the study was that answers to the survey questions given by the participants may have been influenced by their desire to give answers that they believed might advance the goals of the study because of their managements' indirect

involvement. As described somewhere in the study, an official from the office of the Chief of Director at the Ministry of Health was directly involved in the distribution of the survey as the I hand delivered and later picked up (after completion) the survey at the ministry. With the Chief Director being the highest non-political official at a ministry in Ghana, the study participants may experience reluctance to express uncomplimentary responses about their organization. As such, there may be elements of bias toward more positive response, rather than indications of honest feelings. This concern was addressed in the initial stage of the study by way of the informed consent form.

Moreover, the use of purposive (non-probability) sampling is a limitation. While the non-probability sample is not necessarily unrepresentative of the study population, it does mean that it would be a harder for us to know how well this study has helped in our attempt to espouse the extent and the complexity of non-technical security management components in the management of information security in health informatics, as would have been a random sampling.

A number of measures were taken in order to address the limitations and the concerns identified. With regard to the honest responses (resulting from perceived undue influence of the Chief Director), it was initially addressed via the informed consent form. A statement at the beginning of the survey ensured participants that no recognizing information was necessary. Additionally the study participants were assured of confidentiality of their information and they were fully aware that could walk away from the survey whenever they felt uneasiness.

Finally, properly protecting the participants' confidentiality in a study could also be an ethical challenge because of the privacy rights of the participants (Seidman, 2006; Zikmund, 2006). As such, the research data was safely stored under lock and key.

In this chapter, each research question and hypothesis to note the implications of this study, including the implications to information security management in general will be discussed. In addition, prospective limitations and their effects on the results will also be discussed. Finally, recommendations for practical applications of the results conclusions of the study, as well as suggestions for future study will be presented.

Implications

To understand the impact of non-technical factors of organizational culture, security policy, and human behavioral actions and their dimensions on information security management in health informatics, the four research questions in this quantitative study and a discussion concerning the implications of their findings are presented:

Research Question 1: To what extent (if any) is there a relationship between security policy, as measured by user awareness and behavior intention, and Information Security Management, as measured by confidentiality, integrity, and availability?

In summary, the null hypothesis for RQ1 was rejected in favor of the alternative hypothesis. There was a statistically significant, large and positive relationship between security policy as measured by user awareness and behavior intention, and Information Security Management, as measured by confidentiality, integrity, and availability. Security policy accounted for 37.2% of the adjusted variance in ISM scores. There were also significant zero-order correlations between the user awareness and behavior intention sub-domains of security policy, and the ISM sub-domains of confidentiality, integrity and

availability. Multivariate analysis revealed the both user awareness and behavior intention were significant predictors of the ISM sub-domains. This could be interpreted that, when employees are made aware of the specificities within the security policy, they not only follow the policy but do intend helping others to respect the information security policy as well.

Indeed, the first step towards achieving comprehensive ISM through information security policies. Information security policies and practices in organization are based on the ISO/IEC 17799:2005- a framework provides opportunities for organizations and governments to attain compliance and reduce the level of security breaches. Because control of information begins and ends with people (Aytes & Connolly, 2004), it is therefore imperative for both information systems practitioners and policy makers alike to recognize that security awareness and training programs should be designed largely with considerations of users' behavior.

The implication of this research, along with the findings in the literature review was that stakeholders should make it a point to ensure that persons know what is expected of them in terms of data protection (Fedor et al., 2006), else they may be tempted to act in a way they feel is appropriate. Dinev and Hart (2006) described information systems security awareness as the central construct in the formation of user behavioral intentions with regard to technologies. Von Solms and Von Solms (2005) warned that, without proper awareness and training of written security policy, individuals may unintentionally damage or lose data due to the fact that they may not know how they should properly handle such sensitive data. It is therefore critical for policy makers and security professionals to identify end user perceptions, intentions and behaviors as critical elements

for understanding how to move forward with information systems security (Colwill, 2010; Kraemer et al., 2009; Siponen et al., 2007). The findings of the study may further develop research focused on the strength of information security policy in terms of the initial measure that must be in place in the comprehensive management of organization's information resources. Furthermore, this study contributed to academic literature because the study demonstrated a correlation between information security management and security policy.

Research Question 2: To what extent (if any) is there a relationship between organizational culture, as measured by leadership support and normative beliefs, and Information Security Management, as measured by confidentiality, integrity, and availability?

The alternative hypothesis for RQ2 was supported and thus the null hypothesis was rejected. There was a large, positive, statistically significant correlation, $r = .751$ ($p < .001$) between ISM and organization culture. Furthermore, the result of the scatter plots between the ISM and organizational culture with linear regression line ($R = .751$ ($p < .001$), $Y = .836 + .812x$, $R^2 = .565$, $\text{Adj. } R^2 = .562$) suggest a positive correlation. Also, there were statistically significant and large correlations (i.e., above .6) between each of the sub-domains of ISM and leadership support. Organizational culture accounted for 56.2% of the adjusted variance in information security management (ISM) scores. Furthermore, there were significant correlations between the two sub-domains of organizational culture, and the three sub-domains of ISM. When the sub-domains were considered in multivariate analysis simultaneously, it was observed that leadership support was a significant predictor of the sub-domains of ISM, whereas normative beliefs were not

significantly predictive of ISM sub-domain scores over and above that accounted for by leadership support.

The implication of literature and this study was that policy makers and information security practitioners should seek to better understanding of organizational culture to ensure that policies and programs being proposed for deployments do not become still and thus immaterial to evolving information security matters being faced in the organization. It should be noted that, successful implementation of security programs are based on the support of top leadership in the organization. This is because two of the key constituents of security management are culture and policy implementation, as such, vigorous participation and support of top management is required in order to achieve effective security strategy. Knapp et al (2009) suggested that, it is only with top leaderships' total assurance, support and participation in all facets of security management that effective security could be achieved in organizations.

Furthermore, normative beliefs may arise due to an organizational culture security. As such, behaviors can be influenced by both inherent and extrinsic instigators such as apparent behavior of management (Herath & Rao, 2009). A security culture mechanism must be put in place to direct employees conduct organizations. Without such mechanism, employees could well relate with information assets in manners that may lead to risky behavior (Herath & Rao, 2009; Kritzingler & von Solms, 2005); a situation that could cause damage to organizations' information assets.

Research Question 3: To what extent (if any) is there a relationship between human behavior actions, as measured by compliance behavior and deterrent

countermeasures, and Information Security Management, as measured by confidentiality, integrity, and availability?

The null hypothesis associated with RQ3 was rejected. The relationship between human behavior actions and Information Security Management was positive and significant, $r=.646$ ($p<.001$). Linear regression indicated that human behavior actions accounted for 41.4% of the adjusted variance in ISM scores. The result for the three sub-domain scores of ISM showed moderate, statistically significant correlations ($\sim.4$) between the compliance behavior and deterrent countermeasures. There were positive multivariable effects between compliance behavior ($p=.001$) and for deterrent countermeasures ($p<.001$) on three domains of ISM. Also, compliance behavior and deterrent countermeasures were both positively predictive of all three ISM sub-domains of confidentiality, integrity, and availability (all p values $<.001$), even though the variance explained was greater for deterrent countermeasures than for compliance behavior.

The results confirmed past studies that human behavior action has unimaginable influence on organizations' information security management (Ashenden, 2008; Carroll, 2006; Herath & Rao, 2009; Karemer et al., 2009). The results imply that organizations face more complex security challenge now than was acknowledged. The challenge, according to Ashenden (2008), is how to manage human behavior in while trying to achieve optimal resources structure. Thus in order for organizations to formulate strategies in tackling security issues, human behavior must be studied in detail-within the context of security management. Findings of for Research Question 3 confirmed that deterrent countermeasures such as sanctions and security policies should be used as reminders to users to allay potential system abuse. By so doing, non-compliance behavior

of users, which has been found to have an influence on end user's security behavior (Theoharidou et al., 2005), would be checked in order to achieve effective information security management.

Research Question 4: To what extent (if any) do the non-technical security management factors of security policy (measured by user awareness and behavior intention), organizational culture (measured by leadership support and normative beliefs), and human behavior actions (measured by compliance behavior and deterrent countermeasures) predict Information Security Management (measured by confidentiality, integrity, and availability)?

The results for Research Question 4 indicated that the null hypothesis was rejected and alternative hypothesis was supported. The parameter coefficients from the multiple regressions of ISM on the IVs indicated a statistically significant, $F(3, 170)=83.524$, $p<.001$. The non-technical factors predicted 58.9% of the adjusted variance in ISM scores. That is, the non-technical security management factors of security policy, organizational culture, and human behavior actions, were significantly predictive of Information Security Management, as measured by confidentiality, integrity, and availability. Examination of the individual parameter statistics showed that both organizational culture and human behavior action attracted higher predictors of ISM than security policy. Analysis of the sub-domain scores revealed that leadership support sub-domain of organizational culture, as well as deterrent countermeasures sub-domain of human behavior actions were most predictive of ISM scores.

The implication of the findings for RQ4 was that, the non-technical components of information security management do have huge impact on how effective organizations'

information security strategy is formulated. As explained in previous studies (Chang & Lin, 2007; Da Veiga & Eloff, 2009; Sipoen et al., 2010), failure by information security practitioners and policy makers to incorporate any of the non-technical factors in organization's security formulation strategy could lead to undesirable security management outcome for the organization.

Recommendations

Recent research on non-technical factors issues in information security management, as well as the dissertation's design limitations, suggested an assortment of imperative prospects for future research. This study result revealed that there were significant impacts of non-technical factors, including security policy, organizational culture, and human behavior action, on the effectiveness of implementing ISM. Established on the analyses and findings associative with this dissertation research study, the following recommendations were provided:

The result of hypothesis testing of research question one of the study confirmed that security policy as measured by user awareness and behavior intention, has a strong correlation with Information security Management. Past researches have shown that when employees are made aware of (through training) of the security policies, it positively affect their intention to comply with the said policies (Dinev & Hart, 2006; Puhakainen, 2006; Knapp, 2009; Siponen et al., 2010). According to Dinev and Hart (2006), an individual must be aware of information systems security before one could form beliefs about information systems security; which ultimately lead to behavioral intentions regarding information systems security.

Thus based on the findings of this study, it is supported that the impact of human behavior intentions on organizations' security strategy. As such, organizations should endeavor to prioritize the inclusion of non-technical security management factors when designing their overall security strategy. Policy makers and managers in the healthcare sector should put people at the center when writing information security policies by making the end users know what is expected of them in terms of data handling. Failure to have such a comprehensive security policy could lead to a situation where employees would typically act in a way they feel appropriate (Fedor et al., 2006). Having a well thought of written policy would not only outline responsibilities, but would serve as effective deterrents in the overall management of information security.

Research question two of the study expounded that there were significant statistical relationships between organizational culture as measured by leadership support and normative beliefs and ISM. Researchers have extensively written about the importance of social influence (normative and subjective beliefs) in information systems (Da Veiga & Eloff, 2009; Herath & Rao, 2009). Organizational culture is not only the noticeable signals sent by controls, systems, processes and organization structures (Kankanhalli et al., 2003; Schlienger & Teufel, 2005), but also the fundamentals that lie beneath of an organization such as the routines that are followed and the actions being observed on daily basis. It is these actions and norms that form the culture in an organization.

People are more likely to conform with significant others' prospects when those others have the ability to reward the desired behavior (Kritzinger & von Solms, 2005). Therefore, policy makers and top leadership in organizations must change their way of thinking about information security and how it should be managed if they want to improve

their organizations' security outlook. Top management should endeavor to create a culture of information security that would constitute employees' natural way of daily routine. Organizational leaders should work to make certain that they are in harmony with their employees' need to for participation and compliance in relation to creating a workable security culture. It is when management has committed to the organizational culture that effective information security can be achieved in organizations.

Centered on findings of research question three, information systems stakeholders should carefully and fully take into consideration, the human behavior actions when formulating organizations' information security management. The study results revealed a strong relationship between ISM and human behavior action as measured by deterrent countermeasure and compliance behavior. Non-compliance behavior is consistent with conclusions in the technology acceptance literature and has been found to have an influence on end user's security behavior (Theoharidou et al., 2005). Previous studies have shown that large number of issues associated with people exist which could have an impact on an organizations' capacity to manage information security effectively (D'Arcy et al., 2008; Kankanhalli et al., 2003; Straub 1990). As such, organizational leaders and ICT practitioners must consider employees' usability and security behaviors as part of an organization's information security strategy. In addition, stakeholders and information security professionals must determine the potential process control such as deterrent countermeasures to manage user behavior, and their identifiable effects upon that behavior.

Finally, the findings of research question four indicated that the alternative hypothesis for RQ4 was supported; the non-technical factors of security policy,

organizational culture, and human behavior actions, were significantly predictive of Information Security Management, as measured by confidentiality, integrity, and availability. Grounded on the findings and the review of literature, it has become clear that that technical control alone cannot be effective in dealing with security threats. There is the need for information security practitioners and other stakeholders to integrate all of the security components in their attempt to achieve effective security control. Prior researches on information security management, in most cases, have only been on specific issues such as culture, policy, management support, organizational size, etc. due to the perception from the perspective of some researchers that such studies would appear to be methodologically weak (Alfawaz, et al., 2010). Yet, the findings indicated that the real key to an effective information security management is by recognizing the importance of non-technical factors and thus include those factors in the organizations' overall information security strategy. The results of the present study make it clear that future opportunities for further research are warranted. A quantitative method that relied on non-experimental design was applied in this study. More in-depth mixed-mode methods that use a random sampling of participants in the healthcare industry across Ghana would provide a more representative of the entire healthcare stakeholders. Additionally, using both open-ended questions would provide a richer and comprehensive analysis of the research problem. In addition, since this study was conducted through the hard copy (paper and pencil) way, it would be recommended that future research to be conducted via electronic means. Finally, while this study was conducted in Ghana, the findings are not limited to the country of the sub-region. As a consequence, further replicating this study on different populations with varying needs of information security management is

recommended. By furthering the research in other countries, the influence of the research beyond the boundaries used in this study would be greatly enhanced (Creswell, 2009; Trochim & Donnelly, 2008).

Conclusions

This paper examined the impact of non-technical security management factors on information security management in health informatics due to the fact that there is a lack of non-technical security measures in the formulation of information security management (ISM) by stakeholders in health informatics despite humans being at the heart of information technology activities. The study integrated two prominent bodies of research, the theory of reasoned action (TRA) and general deterrence theory (GDT) to formulate the framework. One hundred and seventy seven of a total 200 surveys were responded to.

The results showed that there was strong correlation between non-technical factors (security policy, organizational culture, human behavior actions) and information security management. These findings support and further improve existing research on the connection between ISM and non-technical factors. While there is an overwhelming recognition of the limitation of using only the technical components of security management (Colwill, 2010), there hasn't been many studies on the latter. Most of the information security researches conducted to date has been on specific issues (human behavior, organizational culture, security policy, management support, organizational structure, etc.) only; as against the combined non-technical factors collectively (Alfawaz et al., 2010).

Further research is needed in the area of non-technical component of information security management. Combined with this study, the application of this recommendation

(further research) could provide stakeholders and researchers, a better appreciation of these non-technical factors within information security that could be used for an overall information security management. Another recommendation for future research would be to expand the population of the research because the survey participants in this study were limited to personnel of just two institutions, including healthcare professionals and technocrats in Ghana. A broader random sampling of participants related to healthcare stakeholders would countenance the researcher to better generalize found results to a much larger population.

As security is a collective apprehension among stakeholders, combatting information threats necessitates a comprehensive approach to guarantee that organizations' information assets remain confidential, with impeccable integrity and would always be available for authorized users. Non-technical security measures play an important role in organizations' efforts to protect against accidental mishaps, intentional theft and corruption of data. This research would be of significance to the domain of information security as it extends the knowledge base that currently exists in that field beyond the perception that healthcare stakeholders are not taking the issue of information security seriously. Findings from this study could offer important and potentially new perspective on information security management issues; the growing recognition of the influence of non-technical factors for developing comprehensive information security management, particularly in health informatics security. It is important for information systems practitioners to remember that the most effective countermeasure is not always the technical measure, but a combination of both technical and non-technical elements.

References

- Abor, P. A., Abekah-Nkrumah, G., & Abor, J. (2008). An examination of hospital governance in Ghana. *Leadership in Health Services*, 21(1). doi: 10.1108/17511870810845905.
- Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture : a behavior compliance conceptual framework. In *Australasian Information Security Conference (AISC)*, 2010, Brisbane, Australia. Accessed from <http://eprints.qut.edu.au/29221>.
- Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211. Retrieved from <http://www.courses.umass.edu/psyc661/pdf/tpb.obhdp.pdf>.
- Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26(4), 276-289. doi:10.1016/j.cose.2006.11.004.
- Al-Fakhri, M. O., Cropf, R. A., Higgs, G., & Kelly, P. (2008). E-government in Saudi Arabia: Between promise and reality. *International Journal of Electronic Government Research*, 4(2). doi: 10.4018/ijegr.2008040105.
- Allen, J. H. (2006). *Security is not just a technical issue*. CERT. Retrieved from <https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/management.html>.
- Anastasi, A. & Urbina, S. (1977). *Psychological Testing* (7th ed.). Upper Saddle River, NJ: Prentice Hall.
- Andrew, J. T., & Niels, G. W. (2005). Structural Equation Modeling: Strengths, Limitations, and Misconceptions. *Annual Review of Clinical Psychology*, 1, 31-65. doi: 10.1037/a0020141.
- Asangansi, I. E., Adejoro, O. O., Farri, O., & Makinde, O. (2008). Computer use among doctors in Africa: Survey of trainees in a Nigerian teaching hospital [Electronic Version]. *Journal of Health Informatics in Developing Countries*, 2, 10-14. Retrieved from <http://www.jhidc.org/index.php/jhidc/issue/view/4>.
- Austin, R. D., & Darby, C. A. (2003). The myth of secure computing. *Harvard Business Review*, 81(6), 120-126. Retrieved <http://www.ncbi.nlm.nih.gov/pubmed/12800722>.
- Aytes, K. & Connolly, T. (2004). Computer Security and Risky Computing Practices: A Rational Choice Perspective. *Journal of Organizational and End User Computing (JOEUC)*, 16(3). doi: 10.4018/joec.2004070102.

- Bacik, S. (2008). *Building an effective information security policy architecture*. Boca Raton, FL: CRC Press.
- Bakari, J.K., Tarimo, C.N., Yngstrom, L., & Magnusson, C., (2005). State of ICT security management in the institutions of higher learning in developing countries: Tanzania case study. *Proceedings of the Fifth IEEE International Conference on Advanced Learning Technologies (ICALT'05)*, Kaohsiung, Taiwan, 5-8 July. doi: 10.1109/ICALT.2005.243.
- Baker, W. H., & Wallace, L. (2007). Is information security under control? Investigating quality in Information Security Management. *IEEE Security and Privacy*, 5(1), 36-44. doi:10.1109/MSP.2007.11.
- Barlas, S., Queen, R., Radowitz, R., Shillam, P., & Williams, K. (2007). Top 10 technology concerns (streetwise). *Strategic Finance*. Retrieved from http://www.accessmylibrary.com/coms2/summary_0286-34190620_ITM.
- Basu, S. (2004). E-government and developing countries: An overview. *International Review of Law, Computers & Technology*, 18(1), 109-132. doi: 10.1080/13600860410001674779.
- Blyth, A. & Kovacich, G. (2006). *Information assurance: Security in the information IT security risks*. Woburn, MA: Butterworth-Heinemann.
- Beznosov, K. & Beznosova, O. (2007). On the imbalance of the security problem space and its expected consequences. *Information Management & Computer Security*, 15(5):420–431(12). doi: 10.1108/09685220710831152
- Bishop, M., & Frincke, D. (2005). A human endeavor: Lessons from Shakespeare and beyond. *IEEE Security & Privacy*, 3(4), 49-51. doi:10.1109/MSP.2005.87
- Blobel, B. (2007). Comparing approaches for advanced e-health security infrastructures. *International Journal of Medical informatics*, 76, 454-459. doi:10.1016/j.ijmedinf.2006.09.012.
- Bridges.org. (2006). *Bridges.org, Digital divide*. Retrieved from http://www.bridges.org/digital_divide.
- Browning, J. (2006). Midsize business security spending plans. *Gartner Research*, report G00137654. Retrieved from www.gartner.com/it/products/research/research_services.jsp.
- Brush, M. (2007). MoEIS increases accuracy and efficiency of e-government solutions. *Tier News*. Retrieved from <http://www.tier.com/news/pf.cfm>.

- Burns, N., & Grove, S. (2005). *The practice of nursing research: Conduct, critique, and utilization* (5th ed.). St. Louis, MI: Elsevier Inc.
- Canadian International Development Agency (CIDA). (2008). *Sub-Saharan Africa*. Retrieved from <http://www.acdi-cida.gc.ca/acdi-cida/ACDI-CIDA.nsf/eng/NIC-5595719-JDD>.
- Capogemini. (2006). *Online availability of public services: How is Europe progressing? Web based survey on electronic public services. Web Based Survey on Electronic Public Services Report of the 6th Measurement* (June 2006). Retrieved from http://ec.europa.eu/information_society/europe/i2010/docs/online_pub_serv_5th_meas_fv4.pdf.
- Carroll, M.D. (2006). Information security: Examining and managing the insider threat. *Computer and Information Science*, 156-158. doi: 10.1145/1231047.1231082.
- Center for International Development (CID). (2008). *Readiness for the networked world: A guide for the developing countries*. Information Technologies Group, Center for International Development, Harvard University. Retrieved from <http://cyber.law.harvard.edu/readinessguide/guide.pdf>.
- Central Intelligence Agency (CIA). (2008). *CIA world factbook*. Washington, DC: Author. Retrieved from: <https://www.cia.gov/library/publications/the-world-factbook/geos/sf.html>.
- CERT. (2008). *Vulnerability remediation*. Retrieved from Carnegie Mellon University, Software Engineering Institute web site: <http://www.cert.org/vuls/>.
- Chang, S. H., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3), 345-361. doi: 10.1108/02635570610653498.
- Chen, Y. N., Chen, H. M., Huang, W., & Ching, R. K. H. (2006). E-Government strategies in developed and developing countries: An implementation framework and case study. *Journal of Global Information Management*, 14(1), 23-46. Accessed from <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan028242.pdf>.
- Chetley, A. (Ed). (2006). *Improving health, connecting people: The role of ICTs in the health sector of developing countries. A framework paper*. Infordev. Retrieved from <http://www.infodev.org/en/Document.84.pdf>.
- Chevallerau, F. (2005). The impact of e-government on competitiveness, growth, and jobs. *The IDABC e-Government Observatory of European Communities*. Retrieved from <http://europa.eu.int/idabc/egovo>.

- Ciborra, C. (2005). Interpreting e-Government and development: Efficiency, transparency or governance at distance? *Information Technology & People*, 18(3). doi: 10.1108/09593840510615879.
- Clark, V. L. P. (2010). The adoption and practice of mixed methods: U.S. trends in federally funded health-related research. *Qualitative Inquiry*, 16(6), 428–440. doi: 10.1177/1077800410364609.
- Colwill, C. (2010). Human factors in information security: The insider threat - Who can you trust these days? *Information Security Tech.*, 4(4),186-196. doi:10.1016/j.istr.2010.04.004
- Comerford, J. D. (2006). Competent computing: A lawyer's ethical duty to safeguard the confidentiality and integrity of client information stored on computers and computer networks. *The Georgetown Journal of Legal Ethics*, 19, 629-642.
- Computer Security Institute. (2007). *CSI computer crime and security survey*. Retrieved from <http://www.gocsi.com>.
- Cone, J. D., & Foster, S. L. (2005). *Dissertations and theses from start to finish: Psychology and related fields*. Washington, DC: American Psychological Association.
- Cook, T. D., & Campbell, T. (1979). *Quasi-experimentation: Design and analysis issues for field settings*. Boston: Houghton Mifflin.
- Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Los Angeles: SAGE Publications.
- Cruz-Correiaa, R., Vieira-Marques, P., Costaa, P., Ferreiraa, A., Oliveira-Palharesa, E., Araújo, F., & Costa-Pereiraa, A. (2005). Integration of hospital data using agent technologies - A case study. *Ai Communications*, 18(3), 191-200. IOS Press. Retrieved from <http://iospress.metapress.com/index/F7REAK0RH7V60T0H.pdf>
- Cull, W.L., O'Connor, K.G., Sharp, S., Tang, S. S. (2005). Response rates and response bias for 50 Surveys of Pediatricians. *Health Services Research*, 40 (1), 213–226, doi: 10.1111/j.1475-6773.2005.00350.x
- D'Arcy, J., & Hovav, A. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20, 1 79-98. doi: 10.1287/isre.1070.0160.
- D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM*, 50(10), 113-117. doi:10.1145/1290958.1290971.

- Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management*, 24(4), 361. doi: 10.1080/10580530701586136.
- Da Veiga, A., & Eloff, J. H. P. (2009). An information security governance framework. *Computers and Security*, 29(2), 196-207. doi: 10.1080/10580530701586136.
- Deloitte & Touche. (2007). *2007 Global Security Survey*. Retrieved from <http://www.deloitte.com/dtt/research/ /0,1002,sid=1013&cid=170582,00.html>.
- Denzin, N. K., & Lincoln, Y. S. (2005). *The Sage handbook of qualitative research* (3rd ed.). Thousand Oaks, CA: Sage.
- Dhamija, R., Tygar, J., & Hearst, M. (2006). *Why phishing works*. Proceedings of the SIGCHI conference on Human Factors in Computing Systems. doi.acm.org/10.1145/1124772.1124861.
- Dhillon, H., & Hentea, M. (2005). Getting a cybersecurity program started on low budget. *ACM Proceedings of the 43rd Annual Southeast Region Conference – Volume 1*, Kennesaw, GA, 294-300. doi:10.1145/1167350.1167435
- Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16, 293-314. doi: 10.1111/j.1365-2575.2006.00219.x.
- Dinev, T. & Hart, P (2006). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, 10(2), Winter 2005-6. doi:10.2753/JEC1086-4415100201.
- Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management*, 18(4), 21-39. doi:10.1016/j.cose.2005.09.009.
- Dutta, S., Lanvin, B., & Pua, F. (2004). *The global information technology report 2003-2004: Towards an equitable information society*. New York: Oxford University Press. Retrieved from <http://www.infodev.org/en/Publication.15.html>.
- Dzenowagis, J. (2005). *Connecting for health: Global vision, local insight: Report for the World Summit for the Information Society*. World Health Organization. Retrieved from http://www.who.int/kms/resources/WSISReport_Connecting_for_Health.pdf.
- Ebrahim, Z., & Irani, Z. (2005). E-government adoption: Architecture and barriers. *Business Process Management Journal*, 11(5), 589-611. doi: 10.1108/14637150510619902.

- Eloff, J. H. P., & Eloff, M. (2005). Integrated information security architecture. *Computer Fraud and Security*, 11, 10-16. doi:10.1016/S1361-3723(05)70275-x.
- Ernst & Young. (2007). *10th Annual Global Information Security Survey*. Accessed from http://www.ey.com/global/content.nsf/International/Assurance_&_Advisory_Technology_and_Security_Risk_-_Global_Information_Security_Survey_2007.
- Evans, D., & Yen, D. C. (2006). E-Government: Evolving relationship of citizens and government, domestic, and international development. *Government Information Quarterly*, 23(2), 207-235. doi:10.1016/j.giq.2005.11.004.
- Ezingard, J. N., McFadzean, E., & Birchall, D. (2005). A model of information assurance benefits. *Information Systems Management*, 22(2). doi: 10.1201/1078/45099.22.2.20050301/87274.3.
- Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, 39(2), 175-191. Retrieved from <http://www.psychologie.uni-trier.de:8000/projects/gpower.html>.
- Fedor, D. B., Caldwell, S., & Herold, D. M. (2006). The effects of organizational changes on employee commitment: A multilevel investigation. *Personnel Psychology*, 59(1), 1-29. doi: 10.1111/j.1744-6570.2006.00852.x
- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.
- Fountain, J. (2005). Central issues in the political development of the virtual state. *A paper prepared for The network society and the knowledge economy: Portugal in the Global Context, Lisbon, March 4-5, 2005*. Retrieved from http://www.umass.edu/digitalcenter/research/pdfs/jf_portugal2005_centralissues.pdf.
- Foxcroft, C.D., Patterson, H. Le Roux, D., & Herbs, D. (2004). Psychological Assessment in South Africa: A Needs Analysis. *Final report of the Human Sciences Research Council, Pretoria, South Africa*. Accessed from http://www.commerce.uct.ac.za/Managementstudies/Courses/BUS5033W/2008/Burger%20van%20Lill/Foxcroft-et-al_PsychologicalassessmentinSA.pdf.
- Fraser, H. S. F., Biodich, P., Moodley, D., Choi, S., Mamlin, B. W., & Szolovits, P. (2005). Implementing electronic medical record systems in developing countries, *Informatics in Primary Care*, 14(1), 83-95. Retrieved from <http://groups.csail.mit.edu/medg/ftp/psz/EMR-design-paper.pdf>.

- Frempong, G., Esselaar, S., & Stork, C. (2005). Ghana. In A. Gillwald (Ed.), *Towards an African e-index. Household and individual ICT access and usage across 10 African countries* (pp. 94–105). Johannesburg: Witwatersrand University LINK Centre. Retrieved from <http://link.wits.ac.za/research/e-index.html>.
- Furnell, S. (2006). Malicious or misinformed? Exploring a contributor to the insider threat. *Computer Fraud and Security*, 9, 8-12. doi:10.1016/S1361-3723(06)70419-5.
- Ganczarski, J. Z. (2006). Critical implementation factors in data warehouse implementations in Canadian financial institutions: qualitative expanded study. *Northcentral University Dissertations*. Retrieved May 2, 2008, from the Northcentral University database.
- G.H.S. (n.d.). About Ghana Health Services. *A GHS publication*. Accessed from <http://www.ghanahealthservice.org/aboutus.php?inf=Background>.
- Gordon, L., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). 2004 CSI/FBI ninth Annual Computer Crime and Security Survey. *Computer Security Institute*. Retrieved from <http://www.infragardphl.org/resources/FBI2004.pdf>.
- Hagen, J. M., & Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. *Information Management & Computer Security*, 17(5), 388–407. doi: 10.1108/09685220911006687.
- Hale, J. L., Householder, B. J., & Greene, K. L. (2003). The theory of reasoned action. In J. P. Dillard & M. Pfau (Eds.), *The persuasion handbook: Developments in theory and practice* (pp. 259 – 286). Thousand Oaks, CA: Sage.
- Hanson, W. E., Creswell, J. W., Clark, V. L. P., Petska, K. S., & Creswell, J. D. (2005). Mixed methods research designs in counseling psychology. *Journal of Counseling Psychology*, 52(2), 224–235. doi: 10.1037/0022-0167.52.2.224.
- Heeks, R. (2006). Health information systems: Failure, success and improvisation. *International Journal of Medical Informatics*, 75, 125-137. Retrieved from www.intl.elsevierhealth.com/journals/ijmi.
- Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47, 154-165. doi:10.1016/j.dss.2009.02.005.
- Hersh, W. (2009). A stimulus to define informatics and health information technology. *BMC Medical Informatics and Decision Making*, 9(24). doi:10.1186/1472-6947-9-24.

- Higgins, G. E., Wilson, A. L., & Fell, B. D. (2005). An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture*, 12, 166-194. Retrieved from <http://www.albany.edu/scj/jcpc/vol12is3/featured%20article%202.pdf>.
- Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., & Taylor, R. (2005). Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. *Health Affairs*, 24(5), 1103-1117. doi: 10.1377/hlthaff.24.5.1103.
- Hinsliff, G. (2009). Brown Unveils Plan to Create 100,000 Jobs. UK Prime Minister Gordon Brown's New Year Interview with The Observer, January 4. Available at <http://www.guardian.co.uk/politics/2009/jan/04/gordon-brown-employment-new-deal>.
- Hofstede, G. (2001), *Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations* (2nd ed.). Thousand Oaks, CA: Sage.
- Holloway, I., & Wheeler, S. (1995). Ethical Issues in Qualitative Nursing Research. *Nursing Ethics*, 2(3), 223-232. doi: 10.1177/096973309500200305.
- Hone, K., & Eloff, J. H. P. (2002). Information security policy — what do international information security standards say? *Computers & Security*, 21(5), 402-409. doi:10.1016/S0167-4048(02)00504-7.
- ICT4AD. (2004). *The Ghana ICT for accelerated development policy, Accra, the Republic of Ghana*. Retrieved from <http://www.ict.gov.gh/pdf/Ghana%20ICT4AD%20Policy.pdf>.
- Idowu, P., Cornford, D., & Bastin, L. (2008). Health informatics deployment in Nigeria. *Journal of Health Informatics in Developing Countries*, 2, 15-23. Retrieved from <http://www.jhidc.org/index.php/jhidc/issue/view/4>.
- Ifinedo, P. (2005). Measuring Africa's e-readiness in the global networked economy: A nine-country data analysis. *The Electronic Journal of Information Systems in Developing Countries*, 1(1), 53-71. Retrieved from <http://www.ejisdc.org/ojs2/index.php/ejisdc/article/view/219/184>.
- IICD. (n.d.). Information and communication technology in Ghana. *International Institute for Communication and Development (IICD) online publication*. Retrieved from <http://www.iicd.org/countries/ghana>.
- International Data Corporation (IDC). (2007). *Information society index: An IDC report series*. Retrieved from www.idc.com/getdoc.jsp?containerId=IDC_P7066.

- International Institute for Communication and Development (IICD)*. (2009). Retrieved from <http://www.iicd.org/countries/ghana>.
- Internet World Statistics. (2009). *Internet usage statistics: World internet users and population stats*. Retrieved from www.internetworldstats.com/stats.htm.
- International Organization for Standardization (IOS) (2007). *ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information Security management*. Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297.
- ISO/IEC 17799:2005 (2005). *Information technology – Code of practice for information security management, 2005, ISO/IEC*.
- Kletee, H. (1975). Some minimum requirements for legal sanctioning systems with special emphasis on detection. In A. Blumstein, J. Cohen, & D. Nagin (Eds.), *Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates* (pp. ??-??). Washington, DC: National Academy of Sciences.
- Knapp, K. N., Morris Jr., R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, 28(7), 493-508. Retrieved from <http://dx.doi.org/10.1016/j.cose.2009.07.001>
- Ko, M., Osei-Bryson, K. M., & Dorantes, C. (2009). Investigating the impact of publicly announced information security breaches on three performance indicators of the breached firms. *Information Resources Management Journal*, 22(2). doi: 10.4018/irmj.2009040101.
- Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, 28(7), 509-520. doi: 10.1016/j.cose.2009.04.006.
- Kritzinger, E. & von Solms, S. H. (2005). Five Non-Technical Pillars of Network Information Security Management. *IFIP International Federation for Information Processing*, 175, 277-287. doi:(10.1007/0-387-24486-7_21.
- Kros, J. R., Foltz, C. B., & Metcalf, C. L. (2004/2005). Assessing & quantifying the loss of network intrusion. *Journal of Computer Information Systems*, 45(2), 36-43. Accessed from <http://connection.ebscohost.com/c/articles/15985120/assessing-quantifying-loss-network-intrusion>.
- Lee, S. M., Lee, S.G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management*, 41(6), 707-718. doi:10.1016/j.im.2003.08.008.

- Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management and Computer Security*, 10(2), 57-63. doi: 10.1108/09685220210424104.
- Leedy, P. D., & Ormrod, J. E. (2005). *Practical research: Planning and design* (8th ed.). Upper Saddle River, NJ: Pearson-Prentice Hall.
- Lou, G. (2009). E-government, people and social change: A case study in China. *The Electronic Journal on Information Systems in Developing Countries*, 38(3), 1-23. Retrieved from <http://www.ejisdc.org/ojs2/index.php/ejisdc/article/view/511>.
- Lucas, H. (2008). Information and communication technology for future health systems in developing countries. *Social Science & Medicine*, 66(10), 2122-2132. doi:10.1016/j.socscimed.2008.01.033.
- Ma, Q., Johnston, A. C., & Pearson, J. M. (2008). Information security management objectives and practices: A parsimonious framework. *Information Management & Computer Security*, 16(3), 251-270. doi: 10.1108/09685220810893207.
- Madon, S., Sahay, S., & Sudan, R. (2007). E-government policy and health information systems implementation in Andhra Pradesh, India: Need for articulation of linkages between the macro and the micro. *The Information Society*, 23, 327-344. doi: 10.1080/01972240701572764.
- Mathie, A., & Carnozzi, A. (2005). *Qualitative research for tobacco control: A how-to-introductory manual for researchers and development practitioners*. IDRC, Ottawa, ON, CA: IDRC. Retrieved from <http://idl-bnc.idrc.ca/dspace/handle/123456789/31535>.
- Margetts, H. (2005). Smartening up to risk in electronic government. *Information Polity: The International Journal of Government & Democracy in the Information Age*, 10(1/2), 81-94. Retrieved from <http://iospress.metapress.com/content/7ugdgath5wqjth9n/>.
- Martens, D.M. (2005). *Research and evaluation in education psychology: Integrating diversity with quantitative, qualitative, and mixed methods* (2nd ed.). Thousand Oaks: SAGE Publications.
- Martens, D.M., & McLaughlin, J.A. (2004). *Research and evaluation methods in special education*. Thousand Oaks: SAGE Publications.
- Mengiste, S. A. (2010). Analyzing the challenges of IS implementation in public health institutions of a developing country: The need for flexible strategies [Electronic Version]. *Journal of Health Informatics in Developing Countries*, 4(1), 1-17. Retrieved from <http://www.jhidc.org/index.php/jhidc/issue/view/9>.

- Ministry of Communications (MoC) – (n.d.). *Community of Information Centers (CICs) in the age of ICT: Ghana's blueprint for action Accra*. Ghana: Ministry of Communications.
- Ministry of Information (MOI)-Ghana (n.d.). Accessed from <http://www.mino.gov.gh/>.
- Ministry of Health (MoH)- (n.d.). Accessed from <http://www.mohghana.org/index.aspx>.
- Moahi, K. H. (2009). ICT and Health information in Botswana: Towards the Millennium Development Goals (MDGs). *Information Development*, 25(3), 198-206. doi: 10.1177/0266666909340790.
- Moen, V., Klingsheim, A. N., Simonsen, K. F., & Hole, K. J. (2007). Vulnerabilities in e-governments. *International Journal of Electronic Security and Digital Forensics*, 1(1), 89-100. Retrieved from <http://www.inderscience.com/storage/fl10978361112425.pdf>
- Moon, J. M. (2002). The evolution of e-government among municipalities: Rhetoric or reality? *Public Administration Review*, 62(4), 424-433. Retrieved from <http://www.accessmylibrary.com/article-1G1-90119616/evolution-e-government-among.html>
- Ndou, V. (2004). E-Government for developing countries: Opportunities and challenges. *The Electronic Journal of Information Systems in Developing Countries*, 18(1), 1-24. Retrieved from <http://www.ejisdc.org/ojs2/index.php/ejisdc/article/view/110/110>.
- Nelson, S. D., Isom, D. K., & Simek, J. W. (2006). *Information security for lawyers and law firms*. Chicago, IL: ABA Publishing.
- Ojedokun, A. A. (2005). The evolving sophistication of Internet abuses in Africa. *The International Information & Library Review*, 37(1), 11-17. doi:10.1016/j.iilr.2005.01.002
- Olowu, D. (2009). Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa. *Journal of Information, Law & Technology (JILT)*, 1. Accessed from http://go.warwick.ac.uk/jilt/2009_1/olowu.
- Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards information systems security policy compliance*. Proceedings of 2007 Hawaii International Conference on System Sciences, 2007. doi: 10.1109/HICSS.2007.206.

- Ponemon Institute (2010). 2010 Access Governance Trends Survey, April 2010. Accessed from <http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/Aveksa%20Paper%20FINAL%204.pdf>
- Price, J. H., Dake, J. A., Murnan, J., Dimming, J., & Akpaudo, S. (2005). Power analysis in survey research: Importance and use for health educators. *American Journal of Health Education*, 36(4), 202-208. Retrieved from <http://www.eric.ed.gov/PDFS/EJ792820.pdf>.
- Puhakainen, P. (2006). *A design theory for information security awareness*. Retrieved from <http://herkules oulu.fi/isbn9514281144/isbn9514281144.pdf>.
- Rasmussen, M. (2005). Revised ISO 17799 boosts information security management relevance. *Forrester Analyst Reports*. Retrieved from <http://www.csoonline.com/analyst/report3730.html>.
- Quackenbush, S. L. (2010). General deterrence and international conflict: Testing Perfect Deterrence Theory. *International Interactions*, 36(1), 60-85. Accessed from <http://web.missouri.edu/~quackenbushs/cv.pdf>
- Reichertz, P. L. (2006). Hospital information systems-past, present, future. *International Journal of Medical Informatics*, 3(4), 282-299. doi:10.1016/j.ijmedinf.2005.10.001.
- Reijswoud, V. van (2009). Appropriate ICT as a tool to increase effectiveness in ict4d: Theoretical considerations and illustrating cases. *The Electronic Journal on Information Systems in Developing Countries (EJISDC)*, 38(9), 1-18. Retrieved from <http://www.ejisdc.org/ojs2/index.php/ejisdc/article/view/548>.
- Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In David S. Gochman (Ed.), *Handbook of Health Behavior Research*. Vol.1. New York: Plenum Press, pgs. 113-132.
- Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organizational security culture: Extending the end-user perspective. *Computers and Security*, 26(1), 56-62. doi:10.1016/j.cose.2006.10.008.
- Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal*, 39(4), 60-66. Retrieved from http://www.sis.pitt.edu/~dtipper/2825/ISO_Article.pdf.
- Salla, M., Lewin, S., Swart, T., & Volmink, J. (2007). A review of health behavior theories: How useful are these for developing interventions to promote long-term medication adherence for TB and HIV/AIDS? *BMC Public Health*, 7(104). doi:10.1186/1471-2458-7-104.

- Schlienger, T., & Teufel, S. (2005). *Tool supported management of information security culture*. In 20th IFIP international information security conference, Makuhari-Messe, Chiba, Japan. doi: 10.1007/0-387-25660-1_5.
- Shanks, G. D. (2006). *Qualitative research: A personal skills approach* (2nd ed.). Upper Saddle River, NJ: Prentice Hall.
- Simba, D. O., & Mwangi, M. (2004). Application of ICT in strengthening health information system in developing countries in the wake of globalization. *African Health Sciences*, 4(3), 194–198. Retrieved from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2688333/>.
- Siponen, M., Pahlila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, 43(2), 64-71. doi: 10.1109/MC.2010.35.
- Slater, D., & Kwami, J. (2005). Embeddedness and escape: Internet and mobile phone use as poverty reduction strategies in Ghana. *Information Society Research Group (ISRG)*. Retrieved from http://www.dfid.gov.uk/R4D/PDF/Outputs/Mis_SPC/R8232-ISRGWP4.pdf.
- Smith, E., & Eloff, J.H.P. (2005). *A new perspective on Risk Assessment Techniques, Proceedings of the Fifth International Network Conference (INC 2005)*. pp. 227-234. ISBN 960-7475-32-1, 5-7 July 2005, Samos, Greece.
- Solomon, M. G., & Chapple, M. (2005). *Information Security Illuminated (Jones and Bartlett Illuminated)*. Jones and Bartlett Publishers, Inc. Sudbury, MA.
- Sood, S. P., Nwabueze, S. N., Mbarika, V. W. A., Prakash, N., Chatterjee, S., Ray, P., & Mishra, S. (2008). *Electronic medical records: A review comparing the challenges in developed and developing countries*. Proceeding of the 41st Hawaii International Conference on System Sciences-2008. doi: <http://doi.ieeecomputersociety.org/10.1109/HICSS.2008.141>.
- Sorj, B., & Guedes, L. E. (2005). Digital divide: Conceptual problems, empirical evidence and public policies. In J. Hellström (Ed.), *ICT — A tool for poverty reduction. Challenges for development cooperation* (pp. 9–26). Uppsala: The Collegium for Development Cooperation. Uppsala University.
- Southern African Development Community (SADC). (2007). *Member states profiles*. Retrieved from www.sadc.int/member_states/index.php.
- Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, 24, 124-133. doi:10.1016/j.cose.2004.07.001.

- Straub, D. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255-276. doi: 10.1287/isre.1.3.255.
- Straub, D. W., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for information system positivist research. *Communications of the Association for Information Systems*, 13(24), 380-427. Retrieved from <http://aisel.aisnet.org/cais/vol13/iss1/24>.
- Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *Management Information Systems Quarterly*, 22(4), 441-469. Retrieved from <http://www.cis.gsu.edu/~dstraub/Papers/Resume/Straub&Welke1998.pdf>.
- Tan, C. W., Pan, S. L., & Lim, E. T. K. (2005). Towards the restoration of public trust in electronic governments: A case study of the e-filing system in Singapore. In *Proceedings of the 38th Hawaii international conference on system sciences*. doi: <http://doi.ieeecomputersociety.org/10.1109/HICSS.2005.638>.
- Tawileh, A., Hilton, J. & McIntosh, S. (2007). Managing information security in small and medium sized enterprises: a holistic approach. *Computer and Information Science*, 331-339. Accessed from <http://www.tawileh.net/anas//files/downloads/papers/InfoSec-SME-ISSE.pdf?download>
- The Belmont Report (1979): Ethical principles and guidelines for the protections of human subjects and research. *DHEW Publication No. (OS) 78-0012*, Washington, DC 1979.
- Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, 24(6), 472-484. doi: 10.1016/j.cose.2005.05.002.
- Thielst, C. B. (2007). Regional health information networks and the emerging organizational structures. *Journal of Healthcare Management*; 52(3), 146.
- Thornton, D., Gunningham, N. A., & Kagan, R. A. (2005). General deterrence and corporate environmental behavior. *Law & Policy*, 27(2), 262-288. doi: 10.1111/j.1467-9930.2005.00200.x
- Trochim, W. M. K. (2006). *The research methods knowledge base*. Retrieved from <http://www.socialresearchmethods.net/kb/survtype.php>.
- Trochim, W. M. K., & Donnelly, J. P. (2007). *The research methods knowledge base* (3rd ed.). New York, NY: Thomson.

- Tung, F. C., Chang, S. C., & Chou, C. M. (2008). An extension of trust and TAM model with IDT in the adoption of the electronic logistics information system in HIS in the medical industry. *International Journal of Medical Information*, 77, 324–335. doi: 10.1016/j.ijmedinf.2007.06.006.
- US News & World Report. (2009). President-elect Barack Obama on his American recovery and reinvestment plan. Remarks of President-elect Barack Obama as prepared for delivery. *US News & World Report*, January 8. Available at <http://www.usnews.com/news/stimulus/articles/2009/01/08/president-elect-barack-obama-onhis-american-recovery-and-reinvestment-plan.html>.
- Vast, E. (2007). Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare. *The Journal of Strategic Information Systems*, 16(2), 130-152. doi:10.1016/j.jsis.2007.05.003.
- Vaughn, D. (2006). *ICT4D - Linking policy to community outcomes, Partners in micro-development*. Retrieved from <http://www.microdevpartners.org/documents/ICT4DLinkingPolicytoCommunityOutcomesPDF.pdf>.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425-478. Retrieved from <http://www.jstor.org/stable/30036540>.
- Vogt, W. P. (2007). *Quantitative research methods for professionals*. Boston, MA: Pearson/Allyn and Bacon.
- Von Solms, B., & von Solms, R. (2005). From information security to business security? *Computers & Security*, 24(4), 271-273. doi:10.1016/j.cose.2005.04.004.
- Von Solms, S. H. (2005), Information security governance – Compliance management vs. operational management, *Computers and Security*, 24(6), 443-447. doi:10.1016/j.cose.2005.07.003.
- Vroom C., & Von Solms, R. (2004). Towards information security behavioral compliance. *Computers & Security*, 23(3), 191-198. doi:10.1016/j.cose.2004.01.012.
- West, D.M. (2006). Global e-government: A 2006 global e-Government report. Accessed from www.insidepolitics.org/egovt06int.pdf.
- West, D. M. (2008). *Improving technology utilization in electronic government around the world*. The Brookings Institution. Retrieved from http://www.brookings.edu/~media/Files/rc/reports/2008/0817_egovernment_west/0817_egovernment_west.pdf.

- Westerman, M. A. (2006). Quantitative research as an interpretive enterprise: The mostly unacknowledged role of interpretation in research efforts and suggestions for explicitly interpretive quantitative investigations. *New Ideas in Psychology*, 24(3), 189-211. doi:10.1016/j.physletb.2003.10.071.
- WHO. (2006). *WHO, eHealth tools and services: Needs of the member states report of the WHO Global Observatory for e-Health*. Geneva: WHO. Retrieved from http://www.who.int/kms/initiatives/tools_and_services_final.pdf.
- Williams, F., & Boren, S. A. (2008). The role of electronic medical record in care delivery in developing countries. *International Journal of Information Management*, 28(6), 503-507. doi:10.1016/j.ijinfomgt.2008.01.016.
- Woon, I., & Pee, L. (2004). Behavioral factors affecting Internet abuse in the workplace—an empirical investigation. *Proceedings of the Third Annual Workshop on HCI Research in Management Information Systems*. Retrieved from <http://sigs.aisnet.org/sighci/research/icis2004/si>.
- World Bank. (2009). *World Bank 2009 World Annual Report*. Retrieved from http://siteresources.worldbank.org/extar2009/resources/62239771252950831873/ar09_complete.pdf.
- Yuan, Y., & MacKinnon, D.P (2009). Bayesian Mediation Analysis. *Psychological Methods*, Vol 14(4), Dec 2009, 301-322. doi: 10.1037/a0016972.
- Zhang, Y., Xu, Y., Shang, L., & Rao, K. (2007). An investigation into health informatics and related standards in China. *International Journal of Medical Informatics*, 76(8), 614-620. doi: 10.1016/j.ijmedinf.2006.05.003.
- Zhao, J. J., & Zhao, S. Y. (2009). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly*. doi:10.1016/j.giq.2009.07.004.

Appendixes

Appendix A:
Informed Consent

Information and Informed Consent Sheet

TITLE OF STUDY: Examining the Impact of Non-Technical Factors on Information Security Management in Health Informatics

PRINCIPAL INVESTIGATOR: Abbas Imam, PhD. Candidate, email: doc_imam@yahoo.com, phone: 242-786-542 (Local), +615-649-1973(International).
Supervisor: Dr. M. S. Hammoud at mhammoud@my.ncu.edu or +961 71 348383

We are asking you to take part in a research study. The research is part of my doctoral dissertation. This study examines the influence of non-technical aspects of control on management of information security.

You must first review and sign this form below, before you could take part in the study.

Your participation in this study will require completion of the attached questionnaire. This should take approximately 15-20 minutes of your time. Your responses, and personal identifying information will not be collected and all responses shall remain anonymous. You will not be paid for being in this study. This survey does not involve any risk to you. There is no deception in this study.

Although you may not benefit directly in this research study, your participation in this research could lead to finding an important and potentially new perspective on information security management issues.

You do not have to be in this study if you do not want to be. You do not have to answer any question that you do not want to answer for any reason. We will be happy to answer any questions you have about this study. You may contact me or my advisor at the addresses above.

CONSENT TO PARTICIPATE

I have read the above description of the study and understand the conditions of my participation. By signing below, I agree to participate in the study.

(Signature)

(Date)

Appendix B:

CITI Training Certificate

CITI Collaborative Institutional Training Initiative

Human Research Curriculum Completion Report
Printed on 11/23/2010

Learner: Abbas Imam (username: imamiya)
Institution: Northcentral University
Contact Information: 10000 E. University Drive
Prescott Valley, AZ 86314 USA
Department: School of Business and Technology
Management
Phone: 1-888-327-2877
Email: aimam@nstate.edu

Academic Standards IRB Committee:

Stage 1. Basic Course Passed on 11/23/10 (Ref # 5270888)

Required Modules	Date Completed	
Belmont Report and CITI Course Introduction	11/22/10	3/3 (100%)
History and Ethical Principles - SBR	11/22/10	4/4 (100%)
Defining Research with Human Subjects - SBR	11/23/10	5/5 (100%)
The Regulations and The Social and Behavioral Sciences - SBR	11/23/10	5/5 (100%)
Assessing Risk in Social and Behavioral Sciences - SBR	11/23/10	5/5 (100%)
Informed Consent - SBR	11/23/10	5/5 (100%)
Privacy and Confidentiality - SBR	11/23/10	5/5 (100%)
Research with Children - SBR	11/23/10	4/4 (100%)
Research in Public Elementary and Secondary Schools - SBR	11/23/10	4/4 (100%)
International Research - SBR	11/23/10	3/3 (100%)
International Research	11/23/10	1/1 (100%)
Internet Research - SBR	11/23/10	4/4 (100%)
Workers as Research Subjects-A Vulnerable Population	11/23/10	4/4 (100%)
Conflicts of Interest in Research Involving Human Subjects	11/23/10	2/2 (100%)
Northcentral University	11/23/10	no quiz

For this Completion Report to be valid, the learner listed above must be affiliated with a CITI participating institution. Falsified information and unauthorized use of the CITI course site is unethical, and may be considered scientific misconduct by your institution.

Paul Braunschweiger Ph.D.
Professor, University of Miami
Director Office of Research Education
CITI Course Coordinator

Appendix C:
Permission to Adopt Construct I

Imam, Abbas

From: Mikko Siponen <mikko.siponen@oulu.fi>
Sent: Wednesday, November 17, 2010 2:22 PM
To: Imam, Abbas
Cc: Seppo.Pahnila@oulu.fi
Subject: Re: Permission to Adopt Constructs

I see no problems as long you cite the reference. I do know that the IEEE think about the copyright.

On 17.11.2010, at 22.08, Imam, Abbas wrote:

NorthCentral University
10000 E. University Drive, Prescott Valley, Arizona 86314 USA

Dr. M. Siponen
University of Oulu, Finland
email: mikko.siponen(at)oulu.fi

Dr. S. Pahnila
University of Oulu, Finland

Dr. M. A. Mahmood
University of North Texas

Dear Sir/Madam

Re: Permission to Use Constructs

My name is Abbas Imam, I am a doctoral candidate at Northcentral University in Arizona, USA and currently writing my dissertation in e-Government Security and Informatics. The study examines the existence or absence of information security policies of e-Government systems in sub-Saharan Africa (SSA) within the context of health informatics in Ghana.

I came across the constructs from your (with Pahnila and Mahmood) paper *Compliance with Information Security Policies: An Empirical Investigation* published by IEEE in *Computer and Society*, 43(2), 64-71. I believe that this work would have significant value in my studies, and I would like to adopt them for my survey. I am therefore writing to request permission to use those constructs.

In order to permit the expeditious publication of this article, please reply (via email), indicating whether permission is granted, as soon as possible. You will be appropriately credited as required if permission is granted.

Thank you for your time and attention to this request.

Sincerely,

Abbas H. Imam

November 01, 2010

Appendix D:

Permission to Adopt Construct II

Re: Permission
FROM: Ernest S. Chang
TO: Abbas Imam

Tuesday, March 6, 2012 4:28 AM

Dear Abbas,

You are welcome to use the information, including the constructs, described in the article for academic use (e.g., your proposed PhD research). This is a common practice, in terms of adopting or adapting the content of a journal article in the academic world.

Good lucks and enjoy your research.

Prof. Ernest Chang

Tuesday, March 6, 2012 4:28 AM

----- Original Message -----

From: Abbas Imam
To: eschang@dragon.nchu.edu.tw
Cc: aimam@ncu.edu
Sent: Monday, March 05, 2012 3:13 AM
Subject: Permission

Northcentral University
 1000 E. University Dr., Prescott Valley, AZ 86314

Dr. S. E. Chang
 Dr. C-S Lin

Dear Sir/Madam

Re: Permission to Use Constructs

My name is Abbas Imam, a doctoral student at Northcentral University in Arizona USA, and currently writing my dissertation in e-Government and Information Security. The study examines the importance of non-approach approach in comprehensive information security management in Ghana's health informatics.

I came across constructs in your paper (with C-S Lin), *Exploring Organizational Culture for Information Security Management* in *Industrial Management & Data Systems*, Vol. 107, N. 3, 2007, pp. 438-458 and I would like to adopt them in my study. I believe that the constructs would have a significant value in my research. I am therefore writing to ask for your permission to use the constructs.

In order to expedite this process, I respectfully ask that you reply (via email), indicating whether the permission is granted or not. You will be appropriately credited as required if permission is granted.

Thank you for your time and attention to this request.

Sincerely,
 Abbas H. Imam

Appendix E:

Permission to Adopt Construct III

From: Adele da Veiga [mailto:adele.daveiga@vodamail.co.za]
 Sent: Wednesday, December 01, 2010 7:17 AM
 To: Imam, Abbas
 Cc: eloff@cs.up.ac.za
 Subject: RE: Permission use constructs

Abbas,

Thank you for the request to use the constructs in the paper for your survey. Yes, you can proceed to do so and reference us as the source. Good luck.

Kind regards,

Adele da Veiga

Information Security and Risk Management Consultant
 Tel: +27 11 432 2006
 Mobile: +27 83 957 9757
 Fax: +27 11 432 4768

From: Imam, Abbas [mailto:aimam@Tnstate.edu]
 Sent: Friday, November 19, 2010 7:38 PM
 To: adele.daveiga@vodamail.co.za
 Cc: eloff@cs.up.ac.za
 Subject: Permission use constructs

Northcentral University
 10000 E. University Drive, Prescott Valley, Arizona 86314 USA

Dr. A. Da Veiga
 Dr. J.H.P. Eloff

Dear Sir/Madam

Re: Permission to Use Constructs

My name is Abbas Imam. I am a doctoral candidate at Northcentral University in Arizona, USA and currently writing my dissertation in e-Government Security and Informatics. The study examines the existence or absence of information security policies of e-Government systems in sub-Saharan Africa (SSA) within the context of health informatics in Ghana. I came across the constructs from your paper (with J.H.P. Eloff), *A framework and assessment instrument for information* in Computer and Society, March 2010 and published by Elsevier. I believe that this work would have significant value in my studies, and I would like to adopt them for my survey. I am therefore writing to request permission to use those constructs. In order to permit the expeditious publication of this article, please reply (via email), indicating whether permission is granted, as soon as possible. You will be appropriately credited as required if permission is granted.

Thank you for your time and attention to this request.

Sincerely,

Abbas H. Imam

Appendix F:
Permission to Conduct Survey

In case of reply the number
And the date of this
Letter should be quoted



MINISTRY OF HEALTH
P O BOX MB-44
ACCRA

My Ref. No. MOH/GAD/ 4100 2

28th November, 2012

Your Ref. No....

REPUBLIC OF GHANA


MR. ABBAS H. TIAN
(NCU DOCTORATE, CANDIDATE)
1092 RAMBLING BROOK ROAD
NASHVILLE, TN37218

RE: REQUEST FOR PERMISSION TO CONDUCT A SURVEY

We write with reference to your letter dated 22nd November, 2012 to the Chief Director and our letter No. MOH/GAD/DM/09 dated 8th June 2010 from the Minister's office; requesting for permission to conduct a research study on e-health security in Ghana.

As a response, I am directed to convey to you the approval of the Ministry to your request to undertake the said survey.

The Ministry looks forward to fruitful results, Cooperation and Collaboration with you.


E.M. LONGI
DIRECTOR OF ADMINISTRATION
For: MINISTER OF HEALTH

Appendix G:
Survey Questionnaire

TITLE OF RESEARCH STUDY: Examining the Impact of Non-Technical Factors on
Information Security Management in Health Informatics

I. General Demography Information

Please indicate the answers that best describe you

1. What is your gender?
 - Male
 - Female

2. What is your age group?
 - 30 -40years
 - 40 - 50 years
 - 51 -60 years
 - Over 60 years

3. What is your primary profession?
 - Physician
 - Pharmacist
 - Nurse
 - Public or Government Official
 - Other _____

4. What is your level of education?
 - Advance Diploma/HND
 - Bachelor degree
 - MA/MBA
 - PhD or Ed.D

5. How long is your experience with HEALTH INFORMATICS/Health Information system (eg., e-patients record, e-Health)
 - < 1 year
 - 1-3years
 - 4 -5years
 - Over 5 years

II. Information Security Management (<i>Confidentiality, Integrity, Availability</i>)					
<i>Confidentiality</i>	Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
6. My organization enforces security controls (firewall, anti-virus, encryption, etc) to protect sensitive information.	1	2	3	4	5
7. My organization has well implemented security practices to protect important information from being stolen by malicious intrusions (such as break-in, Trojans, and spy-wares).					
<i>Integrity</i>	Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
8. My organization regularly updates information resources and constantly creates backups.					
9. My organization has change management control in place to prevent unauthorized information changes (creation, alternation, and deletion).					
<i>Availability</i>	Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
10. Legitimate authorized users in my organization have access to the company's proprietary information whenever they needed and at anyplace.					
11. There are well established information access control procedures in my organization, to make					

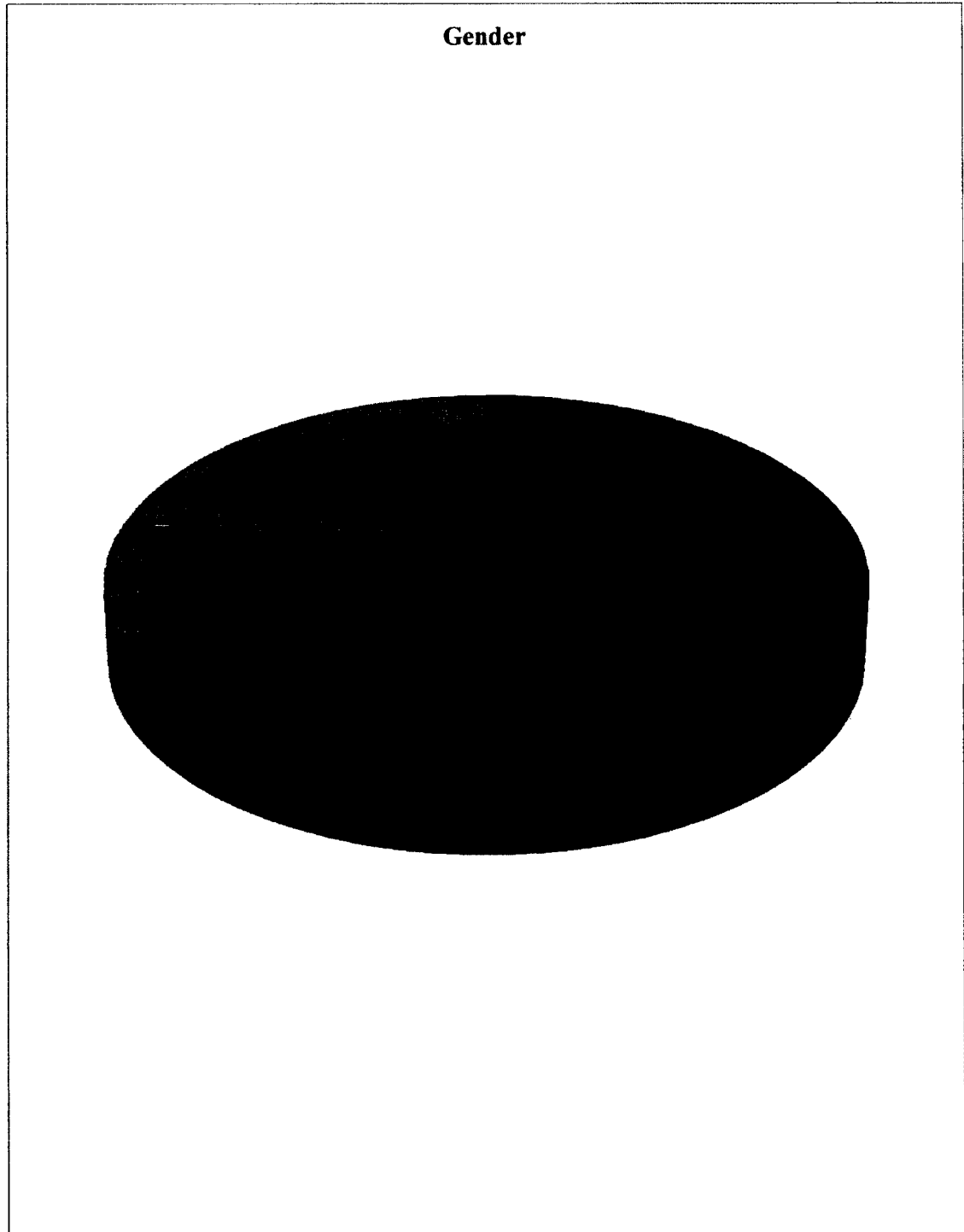
sure that for any particular information resource only authenticated users with right privileges can access such resource.					
III. Information Security Policy (User Awareness and Behavior Intention)					
<i>User Awareness and Training</i>	Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
12. My organization provides training to help employees improve their awareness of computer and information security issues.					
13. My organization has specific guidelines that govern what employees are allowed to do with their computers.					
14. My organization has made training materials available to everyone.					
15. The information security policy in my organization is visibly written.					
<i>Behavior Intention</i>	Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
16. I intend to ignore or circumvent security policies and controls because it is an imposition.					
17. I intend to I play a role in the protection of information within my organization.					
18. I intend to recommend that					

others comply with information security policies.					
19. I intend to assist others in complying with information security policies.					
IV. Organizational Culture (<i>Leadership Support and Normative Beliefs</i>)					
<i>Leadership Support</i>	Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
20. Top management style in my organization is characterized by conformity to good security practices.					
21. Top management considers information security an important organizational significance.					
22. Top management in my organization view information security as part of our overall strategy.					
23. Top management pays ample attention to an information security strategy in order to protect information.					
<i>Normative Beliefs</i>	Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
24. I comply with information security because it is a key norm shared by organizational members.					
25. I comply with information security policies because					

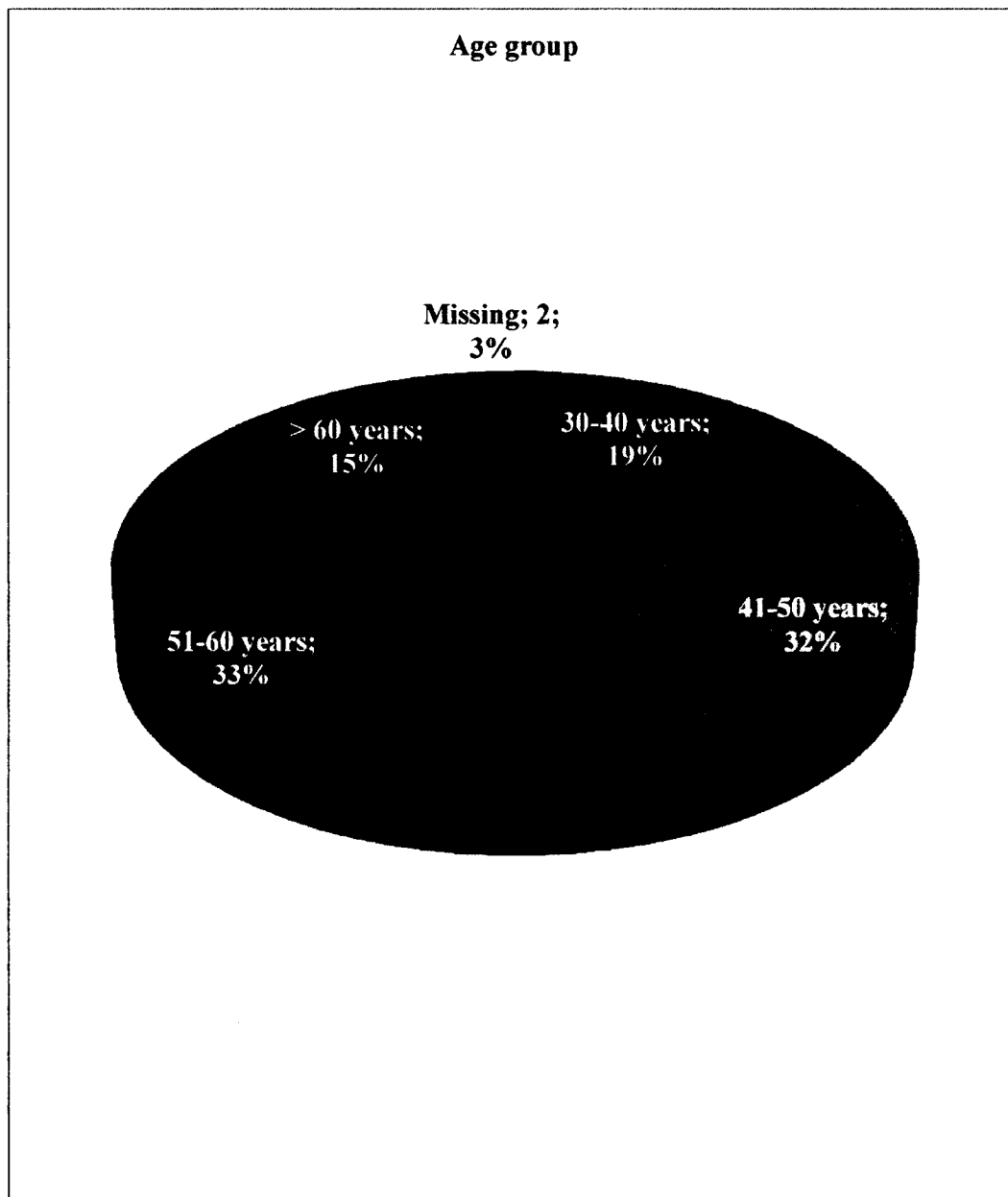
by supervisor wants me to.					
26. I comply with information security policies because my peers also do the same.					
27. I only comply with information security policies due to top management in my organization.					
V. Human Behavior Actions (<i>Compliance behavior and Deterrent Countermeasure</i>)					
<i>Compliance behavior</i>	Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
28. I always comply and lock my work computer screen or a screen saver whenever I leave my desk/office.					
29. My organization monitors any modification or altering of computerized data by employees.					
30. Periodic audits are conducted in my organization to detect the use of unauthorized software on its computers.					
31. My organization monitors employees use of Internet and other social-media sites.					
<i>Deterrent Countermeasure</i>	Strongly Disagree	Disagree	No Opinion	Agree	Strongly Agree
32. It could be in trouble if I download anything (e.g.,					

applications, upgrades, music, video clips, etc.) from the web without scanning.					
33. I follow the information security policies because of the thought of future consequences.					
34. I could be suspended or dismissed if I breach proprietary data in my organization.					
35. If I do not follow my organization's information security policies, I will be severely penalized.					

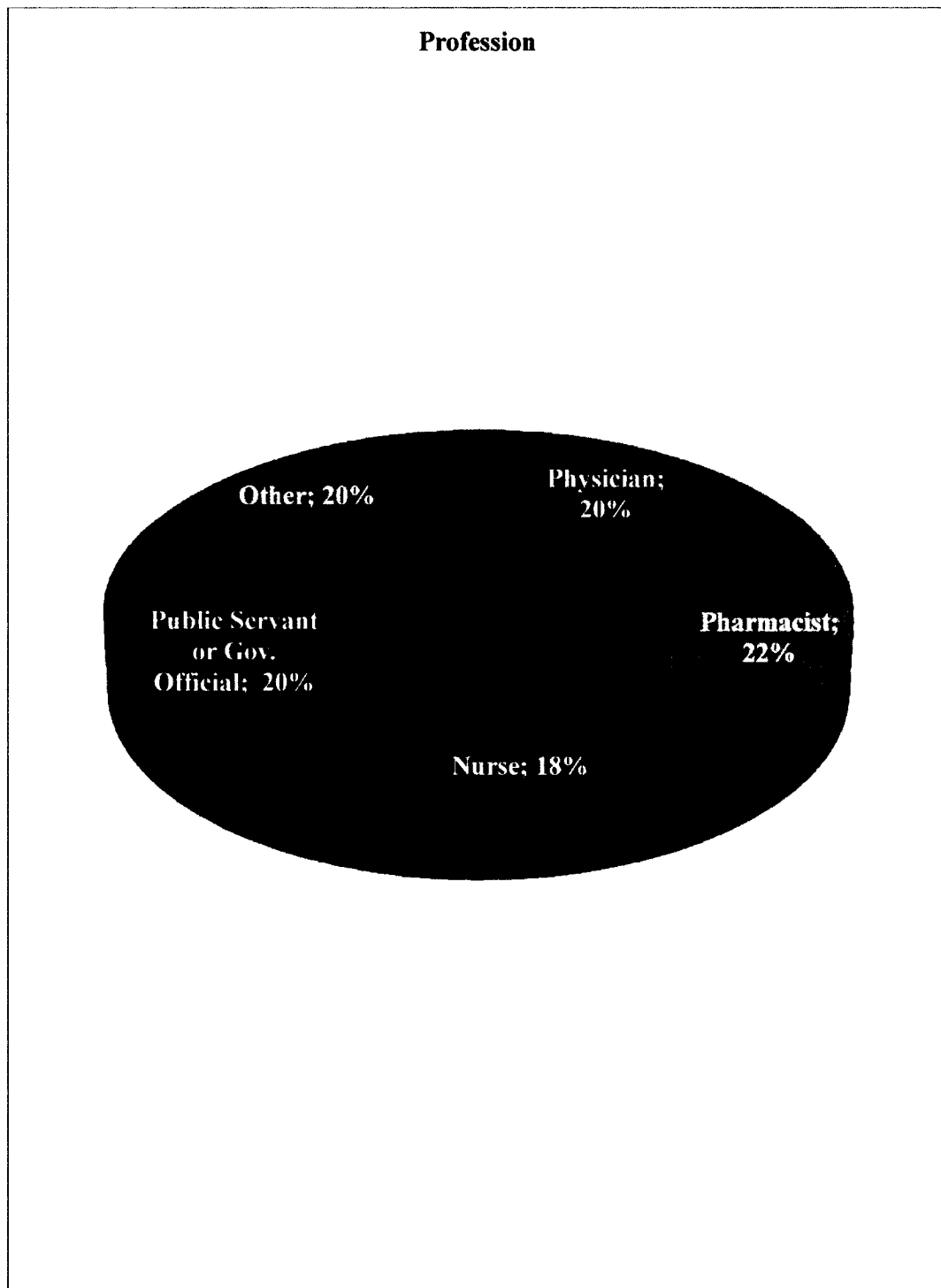
Appendix H:
Participants' Gender



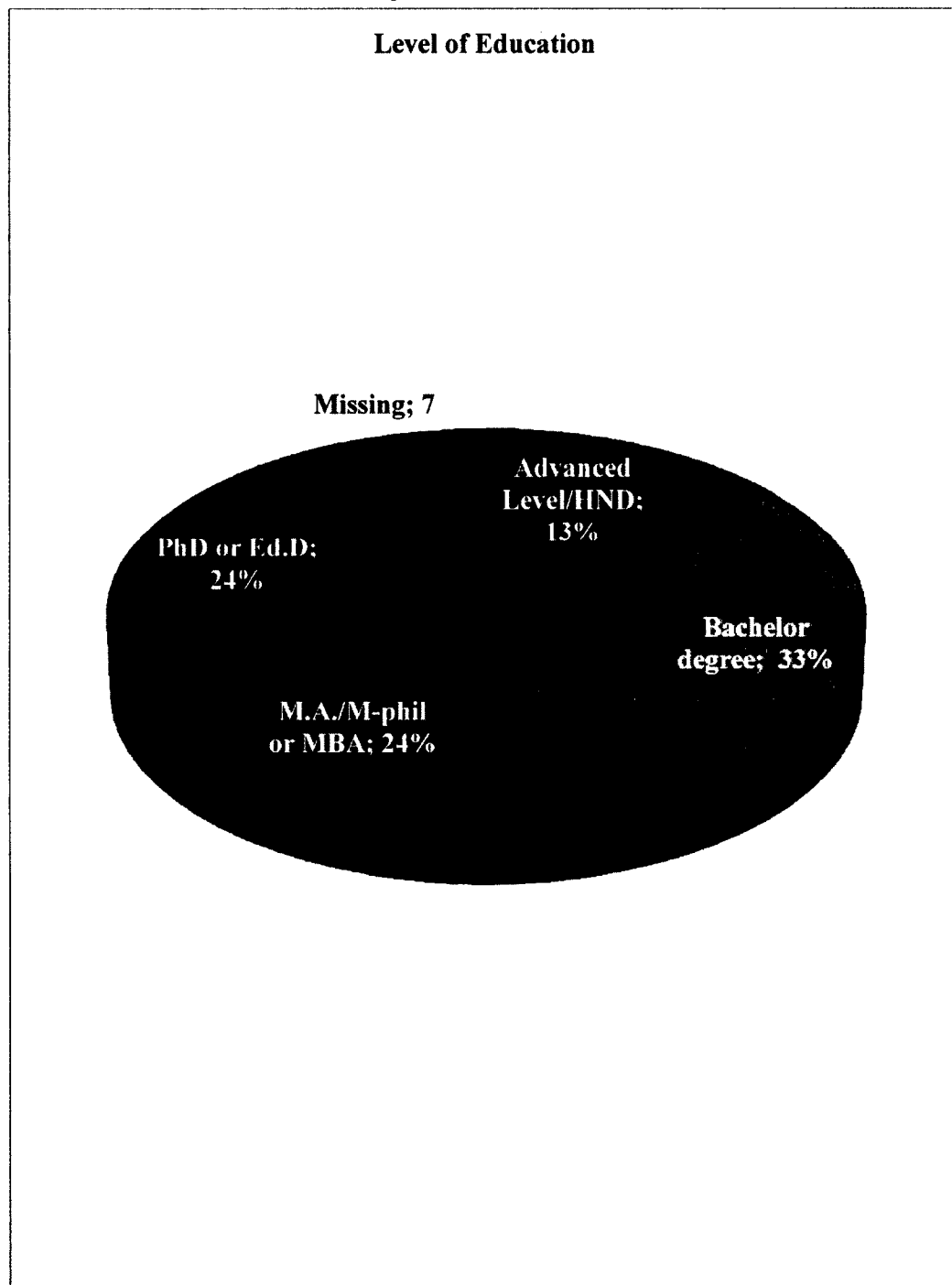
Appendix I:
Participants' Age Group



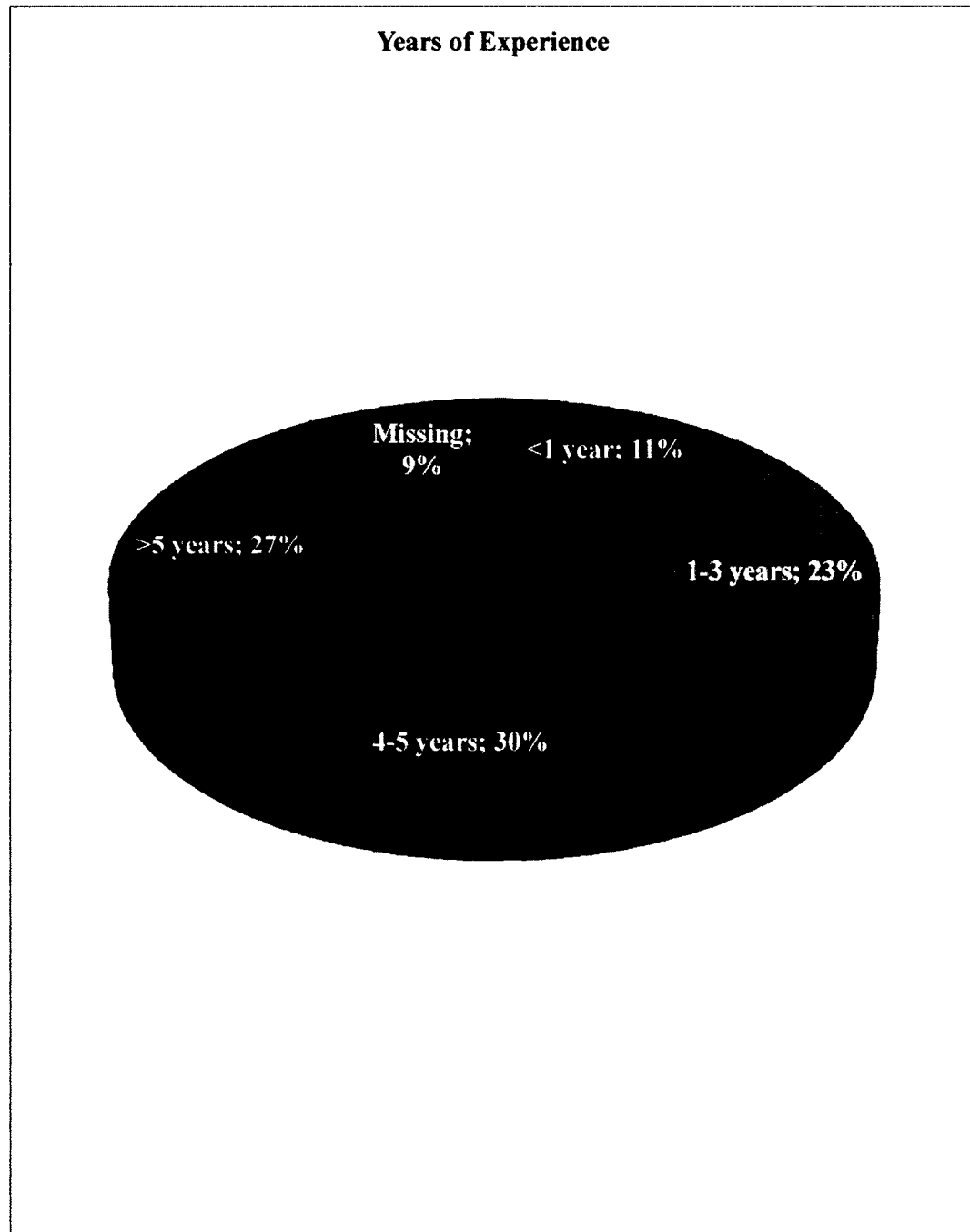
Appendix J:
Participants' Profession



Appendix K:
Participants' Levels of Education



Appendix L:
Participants' Years of Experience



**Appendix M:
Inter-item correlation matrix for Security Policy**

	In my organization awareness training is conducted to help employees (AWARE1)	There are specific awareness guidelines that govern employees computer usage (AWARE2)	Training Materials are made available to all in the organization (AWARE3)	Written InfoSec. policy is visible to all (AWARE4)	I intend to ignore security policy (INTENT) ^a	I intend to play a role in protection of information in my organization (INTENT2)	I intend to Recommend to others to comply with InfoSec. (INTENT3)	I intend to assist others to comply with InfoSec. (INTENT4)
AWARE1	1.000	.347	.294	.391	.339	.281	.270	.261
AWARE2	.347	1.000	.426	.242	-.023	.328	.229	.298
AWARE3	.294	.426	1.000	.301	.150	.111	.244	.347
AWARE4	.391	.242	.301	1.000	.178	.166	.263	.392
INTENT1	.339	-.023	.150	.178	1.000	.299	.265	.177
INTENT2	.281	.328	.111	.166	.299	1.000	.350	.369
INTENT3	.270	.229	.244	.263	.265	.350	1.000	.212
INTENT4	.261	.298	.347	.392	.177	.369	.212	1.000

**Appendix N:
Inter-item correlation matrix for Organizational Culture**

	Management style is characterized by conformity to good InfoSec. Practices (LEAD1)	Management considers InfoSec. significant to the organization (LEAD2)	Management view InfoSec. as part of overall company strategy (LEAD3)	Management pays ample attention to InfoSec. in my organization (LEAD4)	I comply with InfoSec. because it is a norm shared by all in my organization (NORM1)	I comply with InfoSec. because my supervisor wants me to (NORM2)	I comply with InfoSec. because my peers also do the same (NORM3)	I comply with InfoSec. because top management want me to (NORM4)
LEAD1	1.000	.431	.278	.166	.463	.385	.241	.491
LEAD2	.431	1.000	.144	.240	.360	.240	.311	.321
LEAD3	.278	.144	1.000	.312	.264	.489	.299	.390
LEAD4	.166	.240	.312	1.000	.245	.332	.182	.299
NORM1	.463	.360	.264	.245	1.000	.321	.337	.405
NORM2	.385	.240	.489	.332	.321	1.000	.330	.395
NORM3	.241	.311	.299	.182	.337	.330	1.000	.291
NORM4	.491	.321	.390	.299	.405	.395	.291	1.000

Appendix O:
Inter-item correlation matrix for Human Behavior Actions

	I always lock my computer screen or screen saver when I leave my desk (COMPLY1)	My organization monitors any altering of computerized data by employees (COMPLY2)	Audits are conducted to detect any unauthorized software installation on computers (COMPLY3)	Employees' use of internet and other social-media sites are monitored (COMPLY4)	I could be in trouble if I download materials from web on my pc without scanning first (DETER1)	I follow security policy because of fear for future consequences (DETER2)	I could be suspended or dismissed for breach of proprietary data in my organization (DETER3)	I could be penalized if I don't follow security policies in my organization (DETER4)
COMPLY1	1.000	.203	.277	.125	.131	.159	.269	.118
COMPLY2	.203	1.000	.080	.158	.128	.103	.113	.234
COMPLY3	.277	.080	1.000	.224	.141	.202	.221	.145
COMPLY4	.125	.158	.224	1.000	.307	.292	.227	.073
DETER1	.131	.128	.141	.307	1.000	.187	.292	.064
DETER2	.159	.103	.202	.292	.187	1.000	.473	.127
DETER3	.269	.113	.221	.227	.292	.473	1.000	.222
DETER4	.118	.234	.145	.073	.064	.127	.222	1.000

Appendix P:
Multiple regression of ISM on the three independent variables

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B		Correlations		Collinearity Statistics		
	B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
(Constant)	.355	.246		1.443	.151	-.131	.841					
Security Policy	.129	.088	.105	1.457	.147	-.046	.303	.612	.111	.071	.461	2.169
Organizational Culture	.574	.086	.531	6.654	.000	.404	.744	.751	.455	.324	.373	2.682
Human Behavior Actions	.240	.083	.205	2.892	.004	.076	.405	.646	.217	.141	.473	2.114

a. Dependent Variable: ISM (Information Security Management).

Regression $F(3,170) = 83.524$, $p < .001$ $R = .772$, $R^2 = .596$, $Adj. R^2 = .589$.