UNIVERSITY OF EDUCATION, WINNEBA

EXAMINING THE EFFECTIVENESS OF ACCOUNTING INFORMATION SYSTEM AND CYBERSECURITY AWARENESS ON CYBERSECURITY PERFORMANCE IN GHANA: A CASE STUDY OF SELECTED UNIVERSAL BANKS IN THE EFFUTU MUNICIPALITY

JOSHUA APPIAH

MASTER OF BUSINESS ADMINISTRATION

2021

UNIVERSITY OF EDUCATION, WINNEBA

EXAMINING THE EFFECTIVENESS OF ACCOUNTING INFORMATION SYSTEM AND CYBERSECURITY AWARENESS ON CYBERSECURITY PERFORMANCE IN GHANA: A CASE STUDY OF SELECTED UNIVERSAL BANKS IN THE EFFUTU MUNICIPALITY

JOSHUA APPIAH
200026557

A dissertation in the Department of Accounting, School of Business, submitted to the School of Graduate Studies, in partial fulfillment of the requirements for the award of the degree of Master of Business Administration (Accounting) in the University of Education, Winneba

OCTOBER, 2021

DECLARATION

Student's Declaration

I, Joshua Appiah hereby declare that this dissertation, except for quotations and references contained in the published works which have all been identified and duly acknowledged, is entirely my original work and has not been presented for the award of a degree or any other qualification in any other university.

SIGNATURE …… DATE ……

Supervisor's Declaration

I hereby declare that the preparation and presentation of this dissertation were done in accordance with the guideline for supervision of dissertation laid down by the University of Education, Winneba

NAME OF SUPERVISOR: MR. SAMUEL GAMELI GADZO (CA)

SIGNATURE…… DATE…….

DEDICATION

This dissertation is dedicated to my lovely Father: Mr. Samuel Appiah, my Mother: Mrs. Janet Appiah, my caring siblings, and Mr. Samuel Gameli Gadzo for their support in diverse ways throughout my study.

ACKNOWLEDGEMENT

My sincere gratitude and appreciation go to my supervisor, who provided invaluable assistance and support in guiding me through the completion of this research. I cannot forget to thank my siblings, respondents, friends, and colleagues for their support and all those who helped me in diverse ways to complete this dissertation successfully.

TABLE OF CONTENTS

Content	Page
DECLARATION	iii
DEDICATION	iv
ACKNOWLEDGEMENT	v
TABLE OF CONTENTS	vi
LIST OF TABLES	ix
LIST OF FIGURES	x
LIST OF ABBREVIATION	xi
ABSTRACT	xii
CHAPTER ONE: INTRODUCTION	**1**
1.0 Overview	1
1.1 Background of the study	1
1.2 Problem statement	5
1.3 Objectives of the study	6
1.4 Research Question	7
1.5 Purpose of the study	7
1.6 Significance of the study	8
1.7 Scope of the study	9
1.8 Delimitation of the study	10
1.9 Limitations of the study	10
1.9 Organisation of the study	11

CHAPTER TWO: LITERATURE REVIEW **13**

2.0 Introduction 13

2.1 Ghana's Financial Industry Structure 13

2.2 Theoretical Review 14

2.3 Empirical Review 17

2.4 Conceptual framework 30

CHAPTER THREE: METHODOLOGY **32**

3.0 Introduction 32

3.1 Research Design 32

3.2 Population of the study 32

3.3 Sampling and Sampling Techniques 33

3.4 Sources of Data 34

3.5 Data Collection Instrument 34

3.7 Structural equation modeling 35

3.8 Theoretical model based on SEM 36

3.9 PLS-SEM results 39

3.10 Internal Consistency Reliability assessment 39

3.11 Ethical considerations 42

CHAPTER FOUR: RESULT AND DISCUSSION **43**

4.0 Overview 43

4.1 Demographic information 43

4.2 Research Objective 1 46

4.3 Research Objective 2 52

4.4 Research Objective 3 53

4.5 Discussion 56

CHAPTER FIVE: SUMMARY, CONCLUSION, RECOMMENDATION AND SUGGESTIONS FOR FURTHER STUDIES 63

5.1 Overview 63

5.2 Summary of the findings 63

5.2.1 Effectiveness of Accounting Information System 63

5.3 Conclusion 65

5.4 Recommendations 66

5.5 Suggestions for further studies 67

REFERENCES 68

APPENDIX 1 77

LIST OF TABLES

Table		Page
1:	Latent and observed variables	38
2:	Reliability and validity of latent construct	40
3:	Correlation among latent variables with square roots of AVEs	41
4:	Demographic Information (41)	44
5:	Effectiveness of Accounting Information System	47
6:	The level of awareness of Cyber Security among the staff of universal banks	52
7:	Structural Path Significance in Bootstrapping	54

LIST OF FIGURES

Figure		Page
1:	A diagram of the structure of the Ghanaian Financial Service Industry	14
2:	A Computerized Accounting System Model	16
3:	Theoretical Model	37

LIST OF ABBREVIATION

AIS	Accounting Information System
BOG	Bank of Ghana
CAS	Computerized Accounting System
CBG	Consolidated Bank Ghana
CSI	Computer Service Institution
FATF	Financial Action Task Force
FRS	Financial Reporting System
GLS	General Ledger System
HND	Higher National Diploma
ICT	Information communication Technology
IT	Information Technology
MRS	Management Reporting System
OECD	Organistion for Economic Co-operation and Development
SMS	Short Message Service
TPS	Transaction Processing System
UNDOC	United Nations Office on Durgs and Crime

ABSTRACT

Financial institutions continue to increase spending on information system to advance business transactions by systematizing present processes as businesses are changing faster with globalization technology to meet the rapid changes in customer demand. Financial institutions especially banks are considered high-profile target firms for cybercrime and cyber threat. This has led the researcher to investigate the effectiveness of Accounting Information System, cybersecurity awareness on cybersecurity performance. The study is of key importance to the selected universal banks in Effutu Municipality (Winneba) as well as other firms in the same sector. The study designs of the study are exploratory and causal research methods. In addition, quantitative method was applied in data collection and analyses. The study gathered primary data through questionnaires and analyzed using Statistical Package of Social Sciences (SPSS) and Smart PLS. The findings of this study indicate that Accounting Information System used by the selected banks is effective in its operation which provides quality service, quality information, and user satisfaction to enable management in its decision making. Also, employees (staff) had a fair knowledge of cybersecurity-related issues, and that effective Accounting Information System, demographic characteristics, and level of cybersecurity awareness affects the firm's cybersecurity performance. The study concludes that the ability of firms to acquire information system that possesses the required information characteristics and recruit staff with fair knowledge and understanding of cybersecurity influences reducing cybercrime-related attacks on the firm's operations. The researcher recommends that management of the banks should make sure any acquired Accounting Information System possesses required information system characteristics. Also, management should take online and system cyber threats as a priority and constantly organize educative and training programs for its staff on cybersecurity-related issues and finally, consider the demographic characteristics in their recruitment processes especially level of education, working experience in a similar sector, and usage of Accounting Information System when seeking for new staff.

CHAPTER ONE

INTRODUCTION

1.0 Overview

Chapter one presents the overview of the study. The initial section of this chapter presents the background of this study which is the effectiveness of Accounting Information System and cybersecurity. This is followed by the problem statement which seeks to situate the problem this study is investigating. This is followed by the research objective and questions the study asks. The significance of the study is presented in the next section followed by the scope and limitations of the study. The last section discusses how the rest of the study has been organized.

1.1 Background of the study

Advancement in technology has Precise to an innovative system of accounting, new models in economics, and businesses transacted on the internet. The advances have lessened the period and rate of the businesses by simplifying to improve transactions (OECD, 2012). Several organisations primarily use the information system to advance proficiency of business events by systematizing present processes. Nowadays, firms and businesses are changing faster with globalization technology, the accounting information system is one and part of this change and development, this change is contingent on the data and information it produces for the internal and external users for decision making, and reliable financial reporting.

The rapid changes in technology and the dynamic nature of the business environment, as well as increasing demand from customers, have transformed the activities of making business at both the technical level and strategic level of the

organization (Damera, Garilli, & Ricciardi, 2013). The success of organizations depends on their ability to respond to changes in the market environment they are operating. Organisations that adopt and implement these innovations are regarded as being of competitive advantage (Alia, Rahman, & Ismail, 2012). In this way, managers strive to ensure that their organisations successfully adapt to such changes. Accounting information systems have been recognized as an effective tool for achieving not only internal changes but also external organisational changes. As such, Modern financial institutions globally employ a wide range of computer applications to perform their daily work. They use email to communicate, search engines to perform research and accounting software to record and analyze financial transactions for decision-making.

Information on accounting activities is thus vital to organisation's existence, survival and growth. A proper and accurate record of these activities is therefore an effective means of generating the required accounting information. Financial institutions keep track of financial and non-financial data that are identified with its daily operational activities. In managing an organization and implementing an internal control system, the role of an accounting information system is very crucial (Nicolau, 2016). Financial institutions are left with no other option than to invest in the latest technology such as Accounting Information Systems (AIS) to satisfy the needs of their customers and compete favorably.

Accounting information software automates the accounting process, enhancing productivity and cutting down expenses. What's more, it tends to be more exact, quicker to utilize, and less subject to error than the manual system. The introduction of the computerized accounting information system led to effective accounting operations for the organizations (Agbim, 2013). In today's automated, interconnected,

worldwide business environment, Computerised Accounting Systems have become the engine of growth in every business. The banking sector is no exception and has undergone profound changes during the past decades. Recently, the financial sector relies on accounting software, cyber-related systems, and networks to conduct many of its operations. This phenomenon has been embraced by banks all over the world including banks operating in Ghana. The adoption and use of cyber systems in the banking sector have made it attractive for criminals to launch cyber-attacks on these systems.

Financial institutions are gradually expanding and have adopted modern ways of banking such as short message service (SMS) banking and electronic transfers. Gordon et al. (2015) affirms that internet-based businesses and organizations can be troubled by security threats and computer incident which can be a serious issue that can affect their business operations. Transaction activities performed by banks have resulted in the amount of data increasing exponentially, which can transform banking as an institution in the coming years in ways that can be difficultly envisaged. The transition to digitalized market economy globally demands organisations to collect huge amounts of data and or information and employ numerous information systems that are subject to data and cyber threats. A threat to an information resource is any danger to which a system may be exposed. The exposure of an information resource is the harm, loss, or damage that can result if a threat compromises that resource. Financial institutions, especially banks are considered to be high-profile targets for cyber criminals hence the need for them to dedicate huge investment into securing their cyber systems. Since they possess and transact huge amounts of money, they become targets of cyber-attacks. There is a thin line between ensuring ultimate

security as well as harmonizing it with efficient and reliable operations devoid of cumbersome procedures for their customers.

Nevertheless, cybercrime activities by hackers can't be overlooked by management without giving critical attention. Since most cybercrimes are carried out to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them. The issue of cybercrime has become a topical issue for most banks now as some fraudsters use dubious means to get access to the bank's E-banking system to commit the crime.

According to a survey of 522 financial institutions in the United States of America by the Computer Security Institute (CSI), there was an average of $500,000 annual loss to cyber fraud or cybercrime per annum (Richardson, 2018). This suggests that cybercrime has become a big threat to the financial industry requiring huge expenditure to prevent or control it. These technologically advanced threats have transformed the way and manner in which financial institutions operate or transact business with their cyber systems. A very common example is the electronic banking (e-banking) system adopted by almost all banking, and most financial institutions. Karanja and Zaveri (2014) affirm that organisation nowadays experience serious security threats due to the speedy increase in both capacity and frequency of nasty attacks on their infrastructures.

In respect to the increased total use of computer systems within financial institutions, one mode of attacking these institutions is through cyber-attacks. Financial institutions are no exception to this phenomenon due to their adoption of Information Communication and Technology (ICT) in their operations. Carr, (2013) opined that, in this technological society, businesses and organisations are encouraged to manage several threats in information technology mechanisms rather than using it

for competitive benefits. To combat such crimes, institutions need to put in place cybersecurity measures to prevent or control them. In addition to protecting the organisational database, preparations should be made to deal with threats that might result in the deferment of uses and to recover from such situations.

1.2 Problem statement

Financial institutions, especially banks are considered to be high-profile targets for cyber criminals hence the need for them to dedicate resources to securing their cyber systems. Since they possess and transact huge amounts of money, they become targets of cyber-attacks. The Financial Action Task Force (FATF) (2020), points to an increase in money laundering and terrorist financing risks stemming from Covid-19-related crime. These crime includes: (1) increased misuse of online financial services and virtual assets to move and conceal illicit funds, and (2) possible corruption connected with governmental stimulus funds or international financial assistance. A policy brief by Media Foundation of West Africa in 2017, indicated that the United Nations Office on Drugs and Crime (UNDOC) identified West Africa as a major cybercrime offending region and further highlighted Ghana has global recognition as a major cybercrime country and has contributed to the global cybercrime lexicon with the word "sakawa" which refers to cybercrime committed by Ghanaian perpetrators.

International e-commerce operators and online merchants including Amazon, PayPal, and other online retail outlets blacklisted Ghanaian residents from the use of credit cards to purchase goods and services online with their credit cards because of cyber fraud. In Ghana, the cybercrime industry has involved unauthorized access to the financial system of firms and individuals by unauthorized parties both internal and

external of the institutions, email fraud, and other forms of crime carried out mainly through internet banking and other localized payment and mobile banking platforms.

Data show that Covid-19-related cyber threats are increasing. For example, Carbon Black (2020), a cyber security company, noted that ransomware attacks had increased 148% in March 2020 over baseline levels in February 2020. Among the different sectors, the finance sector was the top target, with a 38% increase in cyber-attacks against financial institutions. Cybercrime poses a great threat to most organisations especially the financial sector considering the monetary losses, loss of data as well as loss in customer confidence in the ability of financial institutions to protect their information.

A 2018 report by the Bank of Ghana on banking fraud indicated that cybercrime had the highest percentage of attempted fraud which was about 58%. This awareness is however not exclusive to only the banking institutions but also the non-bank financial institutions. To prevent or control cybercrimes financial institutions adopt various mechanisms and strategies. It is however important for financial institutions to safeguard themselves against cybercrimes during their operations.

Hence this study would seek to delve to examine the effectiveness of Accounting Information System, level of cybersecurity awareness, and firm performance using Accounting Information System. This study would however be situated to some selected universal banks listed on the Ghana stock exchange operating in the Ghanaian financial industry.

1.3 Objectives of the study

The objectives of the study are classified as the general objective and specific objectives.

1.3.1 General Objective

The general objective of the study is to examine the effectiveness of accounting information software and cybersecurity awareness on Banks cybersecurity performance in Ghana.

1.3.2 Specific Objective

The specific objectives of the study are to:

1. examine the effectiveness of Accounting Information System usage.
2. assess the level of awareness of Cyber Security among the staff of universal banks.
3. determine the impact of Accounting Information System on Cybersecurity performance.

1.4 Research Question

To achieve the stated objectives for this study, the following questions have to be asked;

1. What is the effectiveness of Accounting Information System usage?
2. What is the level of awareness of Cyber Security among the staff of universal banks?
3. What is the effect of Accounting Information System on cybersecurity performance?

1.5 Purpose of the study

This study is to delve into the impact of Accounting Information System, how effective cybercrime-related threat has been dealt with in the usage of Accounting Information System and has enhancement in performance among Universal Banks.

This would assess the effectiveness of the Accounting Information System and cyber security.

1.6 Significance of the study

In recent years, many studies have examined how organisations are better utilizing Accounting Information System. Almost all operational activities in which an organisation engages require the processing of data into meaningful information for management decisions. Not surprisingly, most organisation including financial and non-financial institution readily admit that they should manage accounting data or information as it play a sensitive role in their daily operational activities. It is, therefore, necessary to assess the effectiveness of Accounting Information System and the impact on the reduction of cybercrime cases. As an academic work, this research has contributed to already existing knowledge in the area of study. This study would act as a source of future reference, even though much has been written on the connection between business strategy and accounting information system (AIS) very little has been done on the effectiveness of Accounting Information System on cybersecurity.

The study is significant also in terms of its contribution to understanding the significance of cyber security risk management in the usage of accounting software in the Ghanaian banking industry. This would enable investors, management, and IT managers to be able to deal with and justify the implementation and evaluation of Accounting Information System. This study would help bank managers to recognize the effective usage of Accounting Software to gain a competitive advantage, protect accounting data, and prevention of related cybercrime threats. Cyber security risk management recommended at the end of the study would also assist the banking industry to gain a competitive advantage in modern banking.

Scholars interested in the development and implementation of accounting data security would also benefit from this research work. Information systems professionals would as well benefit from this research since it has revealed many issues about effective Accounting information system, cybersecurity, and performance. Policy makers would not be left out of the benefit from this research work. It would also help banks to determine the relationship between Accounting Information System and cybercrime threats prevention.

1.7 Scope of the study

The study is time-scaled and it considers staffs of universal banks within the central region precisely Winneba. The study will cover GCB, Zenith Bank, Republic Bank, and CBG. The choice of Winneba is due to its proximity to the researchers' school of study. This particular case study was chosen because it is convenient to the researchers in terms of the researchers' area of residence and the availability of data for the research work.

This also requires the consideration of reflecting how meaningful the themes hold together in providing the expected support for the research. Data is drawn and collected principally from universal banks. The research is centered on Accounting Information System (AIS) while examining what accounting information system is and the effectiveness of Accounting Information System usage. The other aspect to be explored is examining the effectiveness and ability of the adopted Accounting Information System in enhancing performance and level of awareness about cybercrime-related threats to accounting data and information.

1.8 Delimitation of the study

The concept of accounting information and cybersecurity effectiveness is a broad one and as such, the researcher could not hope to have extensively covered all bases related to this subject area. Nonetheless, by narrowing it down to the banking sector and with specific reference to GCB Limited, Zenith Bank, Republic Bank, and CBG, the researcher was able to operate within a concise scope and determine the impact of accounting information system on cybersecurity performance in the banking sector. The Winneba branches of GCB, Zenith Bank, Republic Bank, and CBG was the center for the research work.

1.9 Limitations of the study

The main limitations of this study were constraints of resources, access, and time. The finance and material resource needed for the sample size for this study were inadequate. Even though the banking industry would have been more appropriate, there are constraints of financial resources and unavailability of data as well as materials which made it not possible to undertake a nationwide study. The unwillingness of management of the bank branches to release information would have helped enrich the study and also established a strong validity and reliability.

1.8 Definition of terms

1.8.1 Accounting Information System

An Accounting Information System (AIS) is generally a computer-based method for tracking accounting activity in conjunction with information technology resources (Fontinelle, 2013).

1.8.2 Accounting software

According to Business Dictionary, Accounting Software is computer programs that are used to maintain accounting information, such as QuickBooks and Peachtree. Accounting software is, therefore, application software that may be developed by an organization itself (in-house) or a third party, or a combination of both.

1.8.3 Cybersecurity

Cybersecurity comprises technologies, processes, and controls that are designed to protect systems, networks, and data from cyber-attacks. Effective cybersecurity reduces the risk of cyber-attacks and protects societies, organizations, and individuals from the unauthorized exploitation of systems, networks, and technologies. Cybersecurity is an umbrella concept that encompasses information security and information assurance (Gyun andVasarhelyi, 2017).

1.9 Organisation of the study

Chapter one introduces the study. This includes the background to the study as well as the problem statement which seeks to present the case for the study. This is situated in relevant reports, literature, and prevailing financial cybercrime occurrence. This leads to the objective of the study and the research questions accompanying the objectives. After, a clear significance of the study is presented followed by the scope and limitation of the study which seeks to draw or address the boundaries of the study.

The literature review is presented in Chapter Two, it discusses the critical issues and relevant topics associated with Accounting Information System and Cybersecurity among banks. It seeks to touch on some literature that supports Accounting Information System, empirical studies on Cybersecurity, and some theories which back it. This chapter reviews work done by others within this field of

research. The sources of these studies were from academic journals, published books, and other authorities in the field.

The next chapter presents the methods used for the study. It provides an insight into the methods used to arrive at the results discussed in the study. It includes data and sampling techniques as well as data analysis methods. Chapter four presents the results and discussions from the study. The final chapter (Chapter five), provides a summary, conclusion, and recommendations of the study.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter is devoted to the review of literature. Literature has been reviewed based on the following themes; theories underpinning the study, Ghana's financial industry structure, concept of Accounting Information System, Accounting Information Software system, Accounting Software, use of technology in the financial sector, cybercrime in the financial sector, and cybersecurity in the financial sector

2.1 Ghana's Financial Industry Structure

The Ghanaian financial industry is mainly made up of depository and non-depository-taking institutions. The depository institutions include universal banks and non-bank financial institutions (NBFIs) such as savings and loans and microfinance institutions. The non-depository institution also includes finance houses, forex bureaux, and others. As of 2019, Ghana has a total of 23 universal banks which is a sharp decrease from 37 as of June 2017. This is due to the recent reforms and cleaning up of the banking sector after the minimum stated capital of the banks was raised to GH¢400 Million.

As of June 2017, there were 141 licensed rural and community banks, 564 microfinance institutions, and 37 savings and loans companies (BoG, 2017). Also, there are about 23 and 26 life and no-life insurance companies respectively in Ghana as at Dec 2016. The National Pensions Regulatory Authority has also granted 78 companies to operate as Pension Fund managers as of 2017. Critical to the Ghanaian financial sector is mobile money which is operated via telecommunications operators. Included are MTN Mobile money, Vodafone cash, and Airtel Tigo Cash. These

developments and diversification of the financial sector has been necessitated to satisfy the growing needs of the country and create a system to promote healthy competition. This has also given the opportunity to create avenues where various strata of the population can be reached with financial services.

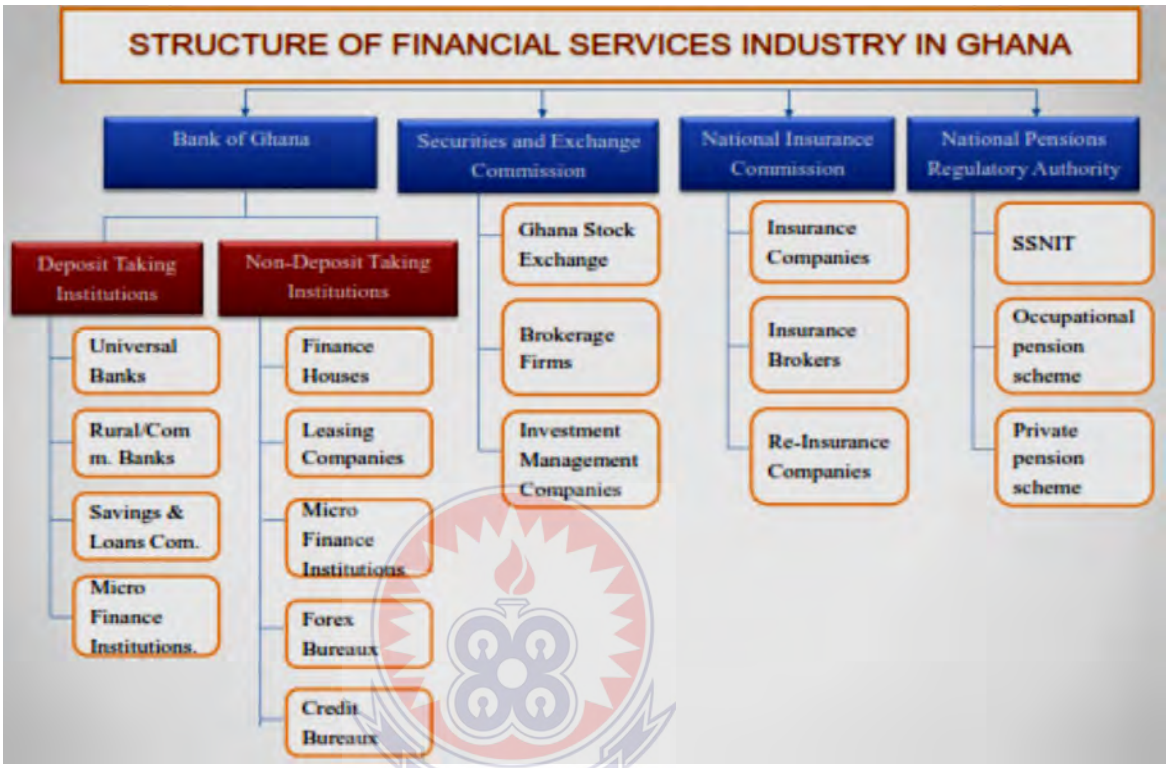


Figure 1: A diagram of the structure of the Ghanaian Financial Service Industry

Source: BOG

2.2 Theoretical Review

This section dealt with the theories that are important to the subject of the study. The theories include system theory and contingency theory.

2.2.1 System Theory

Kaufmann (1966) developed systems to explain historical development as a dynamic process and was more fully developed by biologist Bertalanffy (1968). Bertalanffy argued that everything is interconnected and therefore, we should study interconnectedness as a means of understanding the world. The systems theory

method of analysis involves, first the deconstruction of what is to be explained that is the phenomenon under consideration, secondly, the formulation of explanation that accounts for the behavior of properties of the component separately and finally the synthesis of these explanations into an aggregate understanding of the whole. General systems theory like other innovative frameworks of thought passes through phases of ridicule and neglect. It has benefited, however, from the parallel emergence and rise to the eminence of cybernetics and information theory. Systems theory is relevant to this study because the methods proposed by the theory is to model complex entities created by multiple interactions of components by abstracting from certain details of structure and component and concentrating on the dynamics that define the characteristics functions, properties, and relationships that are internal or external to the system, Computerized Accounting System is a computer-based system, which combines accounting principles concepts as well as the concept of information system to record, process, analyze and produce financial information to its users to make economic decisions (Gorla, Somers and Wong, 2010). The illustrative figure below relates the CAS to systems theory since it involves multiple components which interact to generate usable results these are input, processing storage, users, and output.

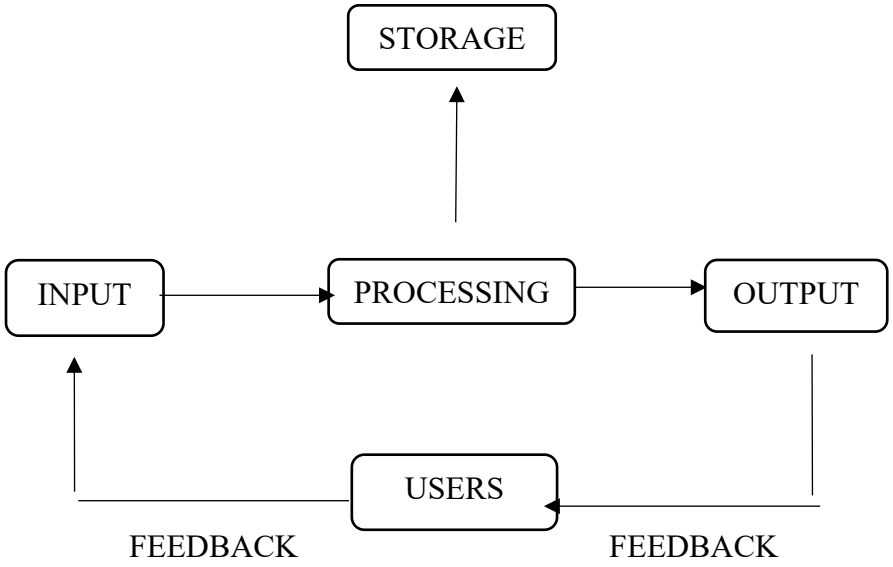


Figure 2: A Computerized Accounting System Model

Source: Gelinas et al. (2005)

2.2.2 Contingency Theory

Since its inception, contingency theory has proposed that organizational effectiveness and efficiency results from the association between organizational characteristics and contingency factors. A literature review identified that some previous research has focused its interest on the study of organizational variables as contingent factors that may influence accounting information systems. Several researchers, such as Nichols and Holmes (1988), Chapellier (1994), Lavigne (2002), and Stepniewski (2008) have identified a significant relationship between contingency factors, the complexity of the accounting information system, and business performance. Choe (1998) argued that the design of an accounting information system can be influenced by contingent variables. These variables are classified into two groups: organizational variables and individual variables. The organizational variables are related to the organizational structure (Chenhall & Morris, 1986; Gerdin, 2005), the task uncertainty (Chong, 1996), the organizational strategy (Naranjo -Gil, 2004), and the budgetary participation (Tsui, 2001). The individual variables refer to

the factors related to some individual characteristics that may have effects on Accounting Information Systems.

The literature review identified the studies by Chapellier (1994), Lavigne (2002), and Ngongang (2007), who selected factors relating to the training, level of education, experience, and age of the leader. These factors have significant effects on Accounting Information Systems. Contingency theory also proposes that organizational performance improves as a result of the interaction between organizational structure and context. In this context, a greater level of fit between the context and the structure leads to better organizational performance (Al-Omiri & Drury, 2007). Some studies opt for this view, which tests the interaction between the contingency factors, the accounting information system, and the performance (Chong, 1996; Naranjo-Gil, 2004; Boulianne, 2007). These studies suggest that there is an interaction between the accounting information system and the factors that influence it. This assumes, however, that these factors are not independent of each other. Companies must allocate their resources to facilitate this interaction.

2.3 Empirical Review

This section discusses the empirical review of both international and local evidence of studies that had been carried out by other researchers.

2.3.1 Accounting Information System Effectiveness

A previous study by Seddon, Graeser and Willcocks (2012) investigated AIS effectiveness in both Europe and the United States. The findings of their study identified the emergence of three groups of constructs that influence AIS effectiveness: 1) systems quality and information quality, 2) perceptual measures on net benefit about AIS use, and 3) AIS behavior. Consistent with Seddon, Graeser, and

Willcocks (2012) stakeholders' perceptions, Elpez and Fink (2010) evaluated AIS success factors in three major Western Australian organizations. Their study developed a model based on user requirements, and findings revealed that information quality and system usability are some of the key influential measures of AIS effectiveness in organisations. Similar evidence was documented in the context of the Iranian oil sector; Ramezan (2009) showed that a significant relationship exists between system quality and information quality with AIS effectiveness. These studies suggested that user perceptions of the quality measures play a significant role in determining the system effectiveness.

Conversely, the absence of the key measures of success might be detrimental to the system success. Bentley, Cao, and Lehaney (2013) argued that low data quality, a lack of system specification, a lack of communication within the system, inflexibility of the systems, and poor system management were causes of AIS ineffectiveness (failure). In addition, Kanungo, Duda, and Srinivas (2010) indicated that facilitating information retrieval, improving product and services quality, and minimizing errors in the functional area have a significate influence on AIS effectiveness. The study revealed that improving system integration is the most influential factor the leads to AIS effectiveness. Fengyi et al. (2010) maintained that effective AIS plays a vital role in enhancing modern organizations, especially in the banking sector through the provision of an integrated value chain system that leads to rapid financing services, excellent fund allocation, and payments, global capital logistic services and cost savings compared to traditional bank accounting information. Also a study by Rodriguez and Spraakman, 2012 indicated that AIS has enhanced the computing power and standardization of organizational activities and,

thus, leads to the provision of more accurate and timely information to the various users in organisations.

Gorla et al. (2010) and Hien et al. (2014) studies indicated that information quality, system quality, and service quality have a significant influence on AIS effectiveness. Basel, Bakar, and Omar (2016) stressed that these three factors were the key ingredients for AIS effectiveness in banks. Thus, AIS is considered an essential managerial decision-making tool capable of handling accounting-related information of the banks (Bonollo, Lazzine, & Merli, 2015). Erna (2015) findings stated that the level of education negatively affected the effectiveness of the use of AIS. Someone who performs the same task repeatedly will keep more things in his memory and can develop a good understanding of the various events of Ariani (2010). Work experience is the period or length of time someone works in an agency, office). The more experience a person has in his field of science, the easier it will be for him to learn new things to improve his performance, this is in line with the research of Ariani (2010) and Adrian (2015) stating the influence of experience has a positive effect on AIS effectiveness Skill is an ability, talent or skill that exists within every human being Adrian (2015).

Raupelien and Stabingis, (2011) study discussed forms and techniques of evaluating the effectiveness of computerized accounting information systems and their potential of utilization and developed a complex model to evaluate the effectiveness of these systems in terms of the technological, economic and social aspects. The study has concluded that characteristics of computerized accounting information systems have a different significance, and can be expressed by quantitative and qualitative measurements, and the success of their use is subject to the correct selection of the system components, including devices, programs,

databases, and highly qualified workers. Besides, the study results specified that the effectiveness of computer-based accounting information systems can be represented in the successful use of these systems in a manner that satisfies the user's requirements.

Al-Hantawi (2010) studies indicated that the most important characteristics that qualify accounting information systems as effective and efficient are the system quality, user satisfaction, service quality, information quality, and speed of processing financial data into accounting information, therefore providing management with the necessary accounting information on time; providing management with the necessary information to perform functions of planning, control, evaluation, speed and accuracy in retrieving stored overall and descriptive information when it is needed; adequate flexibility; general acceptance of workers; simplicity, and to be associated with other information systems in the entity. One of the studies conducted on the Jordanian environment is that carried out by Radaideh (2010). This study has shown that accounting information systems are highly affected by the mechanical processing of data used by the Jordanian Customs Department that mechanical processing technique conforms to a large extent to the requirements of the international auditing standards related to the study of accounting systems and the analysis of the mechanical processing environment. As well, the study shows that the outputs of the used accounting information systems considerably fulfill the requirements and the needs of decisions makers.

Yaseen and Saleh (2014) point out that the evaluation of computer-based information systems used in the Jordanian banks is useful in upgrading their uses and expanding their influence to realize the strategic competitive advantage that is definite for a bank. They emphasize that computerized systems are considered the

technological and organizational basis for more advanced and smart information systems widely integrated with substantive needs of the managements of banks. One such important requirement is to maximize the efficiency of intellectual capital by connecting the best brains of individuals with the most developed information technology. Joudeh, (2010) emphasizes that there are many reasons behind Jordanian banks developing their accounting information systems and increasing their investments in the field of electronic communications technology. They should develop themselves to enter e-commerce methods via the Internet. The most significant reasons are reduction of banking operations service cost, coping with local and international competition, and the fulfillment of clients' needs, and the improvement of customs services. Al-Helo, (2015) has studied the possibility for banks to continue operating or competing in Jordan while not effectively using a computer and communications technology in performing their various activities. He also demonstrated the reality of information and communication systems used in Jordanian banks and concluded that banks cannot continue operating and rendering services to their clients without the use of effective computerized accounting systems.

2.3.2 Accounting information system and Cybersecurity Awareness

A study by Rajan (2010) investigated the relationship between the likelihood of users falling victim to phishing (a form of social engineering which uses emails to maliciously solicit information from computer users, such as login or financial account details) and their awareness of the topic. The study concluded that people fell victim to phishing despite having knowledge and understanding of the importance thereof. This was attributed to incorrect behaviour patterns regarding online security. Mishra (2014) found that many users exhibit a misperception that an installed anti-

virus program is sufficient to prevent compromise of their computers and that a number believe that firewalls are the same as anti-virus applications.

Moreover, a study conducted by Pramod and Raman (2014) found that employees within an organisation are not ignorant of security concerns regarding software applications, but at the same time are not fully aware of all the security risks and necessary security practices. Pretorius and Van Niekerk (2015) recommended training and awareness campaigns after finding vulnerabilities in industrial control systems due to users' insecure password management, unapplied software patches, and outdated or uninstalled anti-virus and malware protection. These studies further illustrate how there can be misalignment among cybersecurity attitudes, knowledge, and behaviour. Furnell et al. (2002) found that organisations and individuals were unsure as to what they should be doing to improve their cybersecurity or how to achieve this, despite acknowledging that it was an issue that needed to be addressed.

In another recent study, socio-demographic characteristics have also been found to have a moderating effect on the cybersecurity behaviors of employees (Anwar et al., 2017). The factor of educational level is not left out totally, as it has been discovered to have some differences with regards to the impact of user's security behaviors (Zhang et al., 2009). Furthermore, in a study that investigated the familiarity of employees with an undergraduate certificate with cyber threats, it was found out that the employees were less familiar with cyber threats (Jeske and Van Schaik, 2017). Kearney and Kruger (2016), argued that the perceptual alignment of diverse groups in an organization is a prerequisite and critical necessity to reach the information security congruence amongst such group of people and implies that different individuals could have distinct perceptions concerning their cybersecurity behaviour. Ogutcu and Chouseinoglon (2016) studies concluded that within

technological institutions there is a marginal increase in the percentage of males dominating managerial roles using Accounting Information System compared to females. Whitty et al. (2015), found that younger people were significantly more likely to engage in the poor security practice of password sharing. Venkatesh, Morris, and Davis (2013) found that age is an important demographic predictor in organizations. To this, the prior research states that increasing age has lower attitudes towards its usage, and acceptance behavior (Igbaria et al. 2011).

Given the significance of cybersecurity to organizations, a fundamental economics-based question has been brought up regularly in prior studies: How much should be invested in cybersecurity-related activities? Gordon & Loeb (2002) presented a model to address this research question, and this model has received considerable attention in the literature, which is known as the Gordon–Loeb Model. The originators argued that because of the information intense characteristics of a modern economy (Internet and the World Wide Web), information security is a growing spending priority for most companies around the world, which prompted them to create an economic model that determines the optimal amount to invest in information security. To be more specific, they stated that the term information security in their model can be interpreted broadly. The Gordon–Loeb Model is applicable to investments related to various information-security goals, for instance protecting the confidentiality, availability, and integrity of information. Hence, the model is also applicable to cybersecurity investments. Their findings indicated that the optimal amount to spend on protecting information sets does not always increase with the level of vulnerability of such information.

The Gordon–Loeb Model can be interpreted as suggesting that the amount that a firm should spend on protecting information sets should generally be only a small

fraction of the expected loss, and accordingly, the findings showed that "managers allocating an information-security budget should normally focus on information that falls into the midrange of vulnerability to security breaches" (Gordon & Loeb, 2002, p. 453). "Since extremely vulnerable information sets may be inordinately expensive to protect, a firm may be better off concentrating its efforts on information sets with midrange vulnerabilities" (Gordon & Loeb, 2002). Moreover, Gordon and Loeb (2016) discussed the Gordon–Loeb Model with a focus on providing insights to aid the model's use in a practical setting. They highlighted that despite its mathematical underpinnings: The Gordon–Loeb Model provides an intuitive framework that lends itself to an easily understood set of steps for deriving an organization's cybersecurity investment level. These four steps are:

I. to estimate the value, and thus the potential loss, for each information set in the organization.
II. to estimate the probability that an information set will be breached based on the information set's vulnerability.
III. to create a grid of all possible combinations of steps 1 and 2 above.
IV. to derive the level of cybersecurity investment by allocating funds to protect the information sets, subject to the constraint that the incremental benefits from additional investments exceed (or are at least equal to) the incremental costs of the investment (Gordon & Loeb., 2016, pp. 57–58).

Similarly, Tanaka, Matsuura, and Sudoh (2005) studied the relationship between vulnerability and information-security investment using data from Japanese municipal authorities. They exploited the Gordon–Loeb Model and suggested that the decision related to information security investments depends on vulnerability. Their findings revealed that the municipal authorities examined did not commit higher-than-usual

expenditures on information security if the vulnerability levels were low or extremely high; however, in contrast, they invested more than usual if the vulnerability levels were medium-high. Therefore, Tanaka, Matsuura, and Sudoh (2005), findings supported the insights provided by Gordon and Loeb's (2002) model. Moreover, Gordon and Loeb (2015) extended the Gordon–Loeb Model to derive the optimal level of investment in cybersecurity activities. They investigated how the existence of well-recognized externalities changes the maximum that a firm should, from a social welfare perspective, invest in cybersecurity activities. They showed that a firm's socially optimal investment in cybersecurity increases by no more than 37 percent of the expected externality loss.

Gordon, Loeb, Lucyshyn, and Zhou (2015), results have important implications for practice because they indicate that unless private-sector firms consider the costs of breaches associated with externalities, in addition to the private costs resulting from breaches, underinvestment in cybersecurity activities is essentially a given. Therefore, the authors concluded that cybersecurity underinvestment might pose a serious threat to national security and the economic prosperity of a jurisdiction. In relation to this, they suggested that "governments around the world are justified in considering regulations and/or incentives designed to increase cybersecurity investments by private sector firms" (Gordon, Loeb, Lucyshyn, & Zhou, 2015b, p. 29).

The latest study by Gordon, Loeb, Lucyshyn, and Zhou (2018) found a significant positive association between the importance that firms attach to cybersecurity for internal control purposes and the percentage of their IT budget spent on cybersecurity activities; accordingly, the study suggests that "treating cybersecurity as an important component of a firm's internal control system serves as an incentive for private firms to invest in cybersecurity activities." The prior literature has also discussed other

approaches to evaluating cybersecurity investments. For instance, Bose and Luo (2014) argued that today's organizations are challenged by the threats of cybersecurity, It is therefore essential for organizations of different sizes and types to understand the potential impacts of cybersecurity on organizational performance. Bose and Luo (2014, p. 204) highlighted that "security investments need to be made by organizations to help secure their tangible and intangible or physical and intellectual assets."

An exploratory study of college students by Mensch and Wilkie (2011) found that a false sense of security, concerning personal information protection, is created by the installation of security applications and tools. Butler and Butler (2014) concluded that South Africans consider convenience a higher priority over security and that only 23% of South African users regularly change their passwords despite 70% indicating that they are aware that this is good practice. These findings show that knowledge does not necessarily translate into good practice. Kaur and Mustafa (2013) investigated how information security awareness of Malaysian small and medium enterprise employees was affected by attitude, behaviour, and knowledge. The study found that attitude and behaviour had significant relationships with information security awareness, but the knowledge did not. This is consistent with the findings of Bada and Sasse (2014).

2.3.3 Cybersecurity Performance

Studies carried by Gordon, Loeb, Lucyshyn, and Sohail (2006) highlighted the impact of cybercrime reduction of information-security threat activities by corporations. They clearly emphasized that management's decision to implement an effective and efficient Accounting Information System had a positive impact on such threat reduction. To clarify, their findings indicated that the reduction disclosure of

information-security threat activities had increased by over 100 percent since the passage of the Sarbanes–Oxley Act when compared with two years before the law's implementation. This was an interesting finding because the Sarbanes–Oxley Act did not explicitly address the issue of information security. On a related note, Gordon, Loeb, and Sohail (2010) examined the voluntary reduction of cyber threats by a corporation with robust effective technological software concerning cybersecurity and argued that voluntary reduction in the annual report on cybersecurity allows a corporation to provide signals to the markets that "the firm is actively engaged in preventing, detecting and correcting security breaches." Accordingly, Gordon, Loeb, and Sohail (2010), suggested that it is a strategic choice whether or not a firm voluntarily decides to disclose items concerning information security; they further asserted that there is clear evidence that an increasing number of organizations are voluntarily disclosing information related to cybersecurity performance. Moreover, Gordon, Loeb, and Sohail (2010) provided empirical support for the argument that performance related to cybersecurity is positively and significantly related to the stock price. Their results indicated generic support for the signaling argument, which states that managers who disclose information concerning cybersecurity response performance are consistent with increasing firm value. Most importantly, their results showed that "voluntary disclosures related to proactive security measures by a firm have the greatest impact on the firm's market" (Gordon, Loeb, and Sohail. 2010, p. 590).

In contrast, Wang, Kannan, and Ulmer (2013) examined the association between the disclosure and the realization of information-security risk and stated that firms often disclose information-security risk factors in public filings. Wang et al. (2013) argued that the internal cybersecurity information associated with performance

may be positive or negative. They evaluated how the nature of the response to security risk factors, believed to represent the firm's internal information regarding information security, is associated with future breach announcements reported in the media. The paper presents a decision tree model, which categorized the occurrence of future security breaches based on the textual contents of the disclosed security risk factors. The authors' model was able to associate disclosure characteristics accurately with breach announcements around 77 percent of the time. Wang et al. (2013) also used text-mining techniques to contribute a richer interpretation of the results. The results showed that the performance of security risk factors with risk mitigation themes is less likely to be related to future breach announcements. Their results indicated that the market reaction following a security breach announcement differs depending on the nature of the preceding cybersecurity performance. To conclude, the study showed that the textual content of security risk factors is an adequate predictor of future reported breaches. More precisely, Wang, Kannan, and Ulmer (2013) demonstrated that firms that respond to actionable (risk-mitigating) information are less likely to be associated with security incidents. The findings indicate that firms taking proactive action have an incentive to disclose their stance on information security truthfully.

In addition, Li and Wang (2018) investigated whether cybersecurity risk performance is informative for future cybersecurity incidents. They focused on two measures: the presence of cybersecurity risk response and the length of cybersecurity risk reduction. They found that the presence of these risk factors in the pre-guidance period and the length of these risk reductions are related to future reported cybersecurity incidents. However, the findings indicated that the association between the presence of cybersecurity risk performance and subsequently announced

cybersecurity incidents become insignificant after the passage of the USA Securities and Exchange Commission's (SEC) cybersecurity disclosure performance guidance. Hence, the work of Li and Wang (2018) supports the SEC's decision on underlining cybersecurity risk performance disclosure. However, Li et al. pointed out that the SEC's disclosure guidance may unintentionally encourage firms to disclose cybersecurity risks regardless of the level of the risks.

Further research, examines how managers react to data security performance. Xu, Guo, Haislip, and Pinsker (2019) explore whether managers are more likely to engage in earnings management following the detection of data security breaches. Their findings suggest that firms are more likely to engage in real earnings management when the breach is related to financial information, the disclosure of the breach is delayed and the information environment is weaker (measured by low analyst coverage). From a different perspective, Banker and Feng (2019) also examined how managers respond to detected data security breaches by examining the association between detected data security breaches and chief information officer (CIO) turnover. The authors argue that computerized information security performance reflects the CIO's information technology (IT) performance. When the CIOs fail to meet this performance expectation (i.e., a breach occurs), the likelihood of turnover will increase. Their findings demonstrate that the breach increase CIO turnover likelihood by 72 percent.

The next study examines the economic impact of cybersecurity breaches. Specifically, Richardson, Smith, and Watson (2019) explore whether cybersecurity breaches impact organizations abnormal returns, future accounting measures of performance, insider sales, and reporting of internal control material weaknesses. Results indicate that, on average, the economic consequences of privacy breaches on

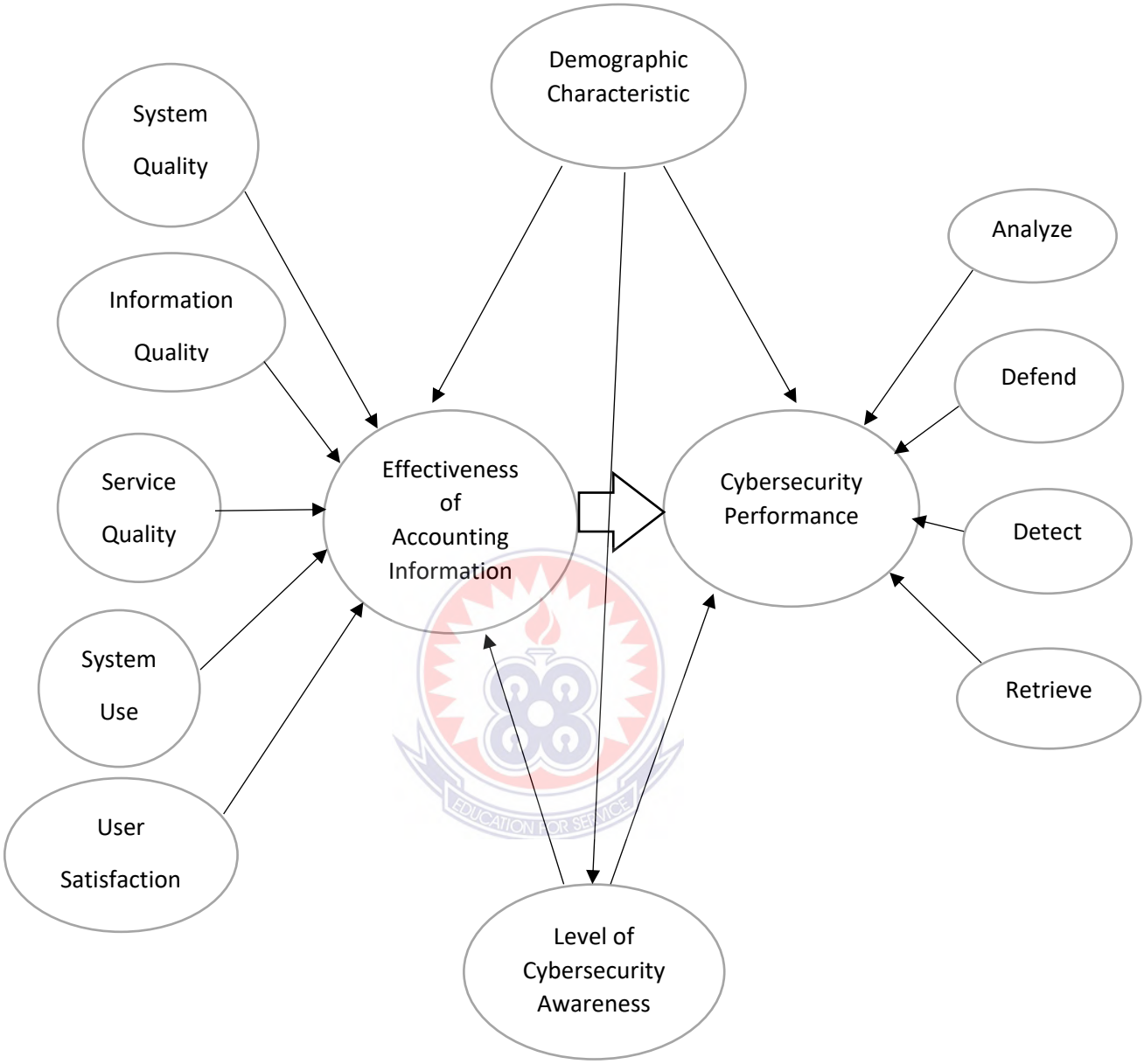
firms' cumulative abnormal returns, future accounting measures of performance such as sale growth return on sales and operating expense, higher audit and other fees, and future Sarbanes Oxley Act 404 reports of material internal control weaknesses are generally very small. Frank et al. (2019) examine whether a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. The authors design an experiment to capture how disclosures proposed by the American Institute of Certified Public Accountants may influence non-professional investors' perceptions. The authors find that issuing a management's report without assurance is more effective when a company has not disclosed a prior cyberattack. Further, issuing an independent cybersecurity assurance report may increase a company's ability to attract investments.

Finally, Cheng and Walton (2019) explore whether the timing and source of data security performance impact investors' reactions to data breaches. By using an experimental setting, the authors demonstrate that investors are less likely to invest in a company if the breach is announced by the company itself, as compared to an outside source. However, timeliness does not seem to be a major factor in whether investors will invest in a company with a high cybersecurity performance (detection and prevention of cyber-crime)

2.4 Conceptual framework

The independent variable for the study is accounting information systems which are enhanced by variables such as system quality, information quality, service quality, system use, and user's satisfaction which is influenced by a moderating variable "level of cybersecurity awareness measures among staff" enforced by the human resource while cybersecurity performance is the dependent variable. The

relationship between the dependent variable and the independent variables was conceptualized in the diagram below.



Source: Author's Conceptual framework (2021)

CHAPTER THREE

METHODOLOGY

3.0 Introduction

This chapter describes the procedures and methods that were used and how questionnaires surveys were undertaken. The chapter outlines the research approach, research design, population of the study, sample size, sampling technique, research instrument, and the tools used for data collection. This section finally describes how field data were made suitable for presentation and analysis and the tools used for data presentation and also describes the area of the study.

3.1 Research Design

According to Malhotra and Birks (2007), a research design is a framework or a blueprint for conducting business research. It specified the detailed procedures necessary for obtaining the information needed to structure or solve business research problems. The research design that was used in this study is exploratory and causal because it makes use of the exploratory design in providing answers to the first and second objectives which sought to provide an insight into the effectiveness of the Accounting Information System and the level of security awareness of staff. The causal research design tries to identify the extent to which or the nature of the cause-and-effect usage and component of accounting information system affects firms cybersecurity performance which seeks to answer the third objective. A quantitative research method and instrument were used to obtain data for analysis in this study.

3.2 Population of the study

A population is any complete group of entities sharing some common set of characteristics (Greenfield, 2016). Given these, the target population of this study

includes the staff of GCB, Zenith Bank, Republic Bank, and CBG. According to staff statistics from the various banks provides a total of 41 staff that uses Accounting Information System at the workplace. The table below provides the statistical breakdown for each bank. This population is chosen due to easy accessibility to data collection. This helped have a representative sample for the study and enabled the researchers to collect objective and detailed information.

Financial Institution	**Number of Staff**
GCB	16
Republic Bank	11
CBG	8
Zenith	6
Total	**41**

3.3 Sampling and Sampling Techniques

In research, the process of sampling made it possible to limit the study to a relatively small portion of the population called sample. The number of people included in the sample made it possible to have a representative sample of the entire population which is accepted in any scientific study. According to Mason et al. (1997), a sample refers to a set of people or objects chosen from a larger population to represent that population to a greater extent. A sample also is a unit or sub-group of the population selected for participation in the study. The characteristics of the sample called statistics were then used to make inferences about the parameters.

The sampling strategy utilized in any research study affects the extent to which the results can be generalized to a wider population; therefore, the sampling strategy has implications in terms of the external validity of the study. This study was

conducted using the census sampling technique. Census sampling techniques were used to generally collect information from each unit of the population for analysis due to the small number of staff members within the selected commercial banks within winneba.

3.4 Sources of Data

According to Saunders et al. (2009), there are two main sources of data, primary data, and secondary data, both of which are used in the study. They define primary data as data that are gathered for the first time for specific research or purpose. While secondary data are data that are collected, which has been published and for which new researchers can rely as a source of information. This is data collected for the problem at hand which includes literature from journals, textbooks, manuals reports, and publications and articles from the internal. For the purpose of this research primary data were collected, since the questions, the researcher asked are tailored to elicit firsthand data from respondents for analysis.

3.5 Data Collection Instrument

There are many techniques of data collection for research work. Some of the methods are questionnaires, observations, documentaries, and analysis among others. Each data collection instrument is more suitable for a specific research strategy (Easterby-Smith, 1991). For the purpose of this study, the researcher made personal contact to administer questionnaires to collect the necessary data for analysis and interpretation. Since the nature of the daily job activities engage by the staff of these Universal Banks of which time wouldn't permit them, the researcher explained each item to enable quick responds to the questionnaire on time. Therefore, questionnaire was employed to collect on hand timely and accurate data based on the research question and objective.

3.6 Data Analysis

After data collection, questions were coded and entered into Statistical Package for Social Sciences (SPSS) then analysis was run to provide answers for research objectives 1 and 2. Objective 1 and 2 data were analyzed using descriptive statistics for quantitative data. Descriptive statistics involve the use of frequencies, percentages, mean and standard deviations. Quantitative data were presented in tables, bar graphs, and pie charts, while explanations to the same were presented in prose (Mugenda & Mugenda, 1999). For research objective 3, the Smart PLS was used to conduct the Structural Equation Model (SEM) to obtain the relationship between the independent and dependent variables.

3.7 Structural equation modeling

Structural equation models (SEMs) offer litheness for testing such models, allowing one to use multiple predictors and criterion variables, construct latent (unobservable) variables, model errors in measurement for observed variables, and test mediation and moderation relationships in a single model (Hair et al. 2012; Bentler, & Huang 2014; Bisbe & Malagueno 2015; Hair et al. 2016). SEM covers all the reflective indicators in one construct. The two types of SEM are Covariance-based structural equation modeling (CB-SEM) and partial least squares structural equations modeling (PLS-SEM) used in research. Because of theoretical and methodological issues, there had been an increase in the use of PLS-SEM compared to that of CB-SEM (Hair, Sarstedt, Pieper, Ringle, & Mena, 2012). According to Kumar and Sujit (2018), variance which predicts construct relationship is explained effectively by PLS-SEM and this method emphasizes maximizing the explained variance of the endogenous latent variables instead of replicating the theoretical covariance matrix. PLS-SEM methodology becomes very useful to conduct predictive analysis with

highly complex data. This methodology estimates latent variables through composites, which are exact linear combinations of the indicators assigned to the latent variables (Nitzl, 2016).

From this backdrop, the Partial least square structural equation modeling methodology (PLS-SEM) was employed to examine the effect of Accounting Information System effectiveness on Cybersecurity performance. . The PLS-SEM methodology was adopted based on the assumption that the demographic characteristics; level of awareness of Cyber Security; Accounting Information System effectiveness and Cybersecurity performance. The researcher used the Smart-PLS software to apply PLS-SEM as this technique effectively handles nonlinear relationships. As a first step in PLS-SEM, missing data imputation is carried out by Stochastic Multiple Regression Imputation algorithm. The latent constructs consist of reflective measurement scale which are interchangeable and must be highly correlated. In the initial assessment of the model, the loadings of all the variable indicators in the constructs is used for scale purification. Any indicator which has less than 0.5 loading is dropped from the model. This means that the indicator is different from the rest and must be dropped. In this study none of the latent variables were dropped.

3.8 Theoretical model based on SEM

The theoretical model (original model) includes an exogenous latent variable and three endogenous latent variables. The exogenous latent variable is a bank-specific variable reflected by four observed variables. The Effectiveness of Accounting Information System latent variable includes system quality (SQ), information quality (IQ), service quality (SerQ), system use (SysQ), and user satisfaction (USQ). The model employs three endogenous latent variables, including

the level of security awareness (LOSA), demographic characteristics (DC), and cybersecurity performance (CP).

Therefore the theoretical model is shown in figure 3.

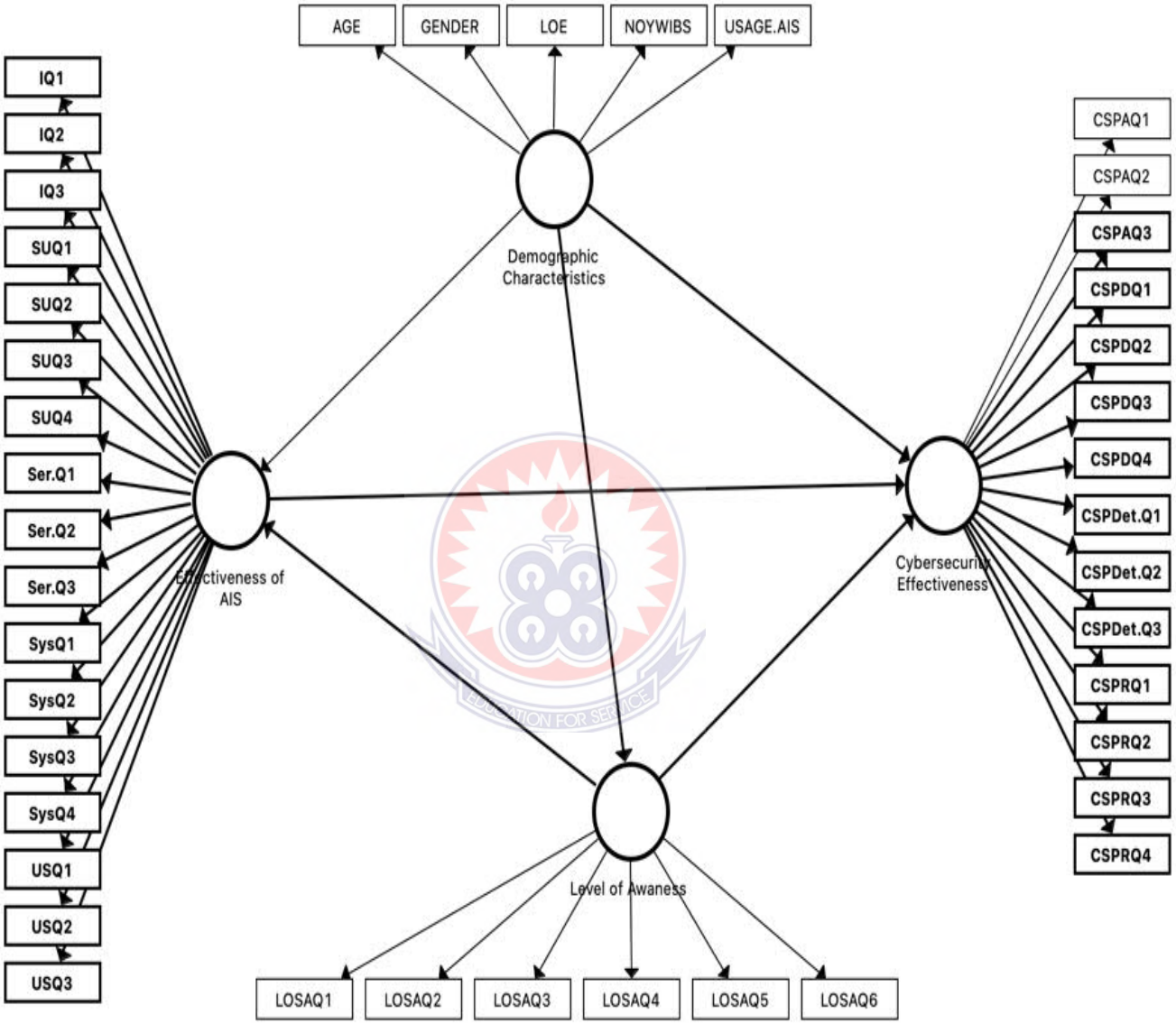


Figure 3: Theoretical Model

Source: Authors construct (2021)

Table 1: Latent and observed variables

Latent Variables	Observed Variables
Effectiveness of AIS (EAIS)	*SQ1*:The system is reliable
	SQ2: The system easy to learn and understand its features
	SQ3: The response time for the system is fast
	SQ4: The system is flexible
	*IQ1:*Management reports are reliable
	*IQ2:*Web pages are accurate and upload
	IQ3: System output are clear
	IQ4: The information from AIS improves the quality of work
	SerQ1: IT team provide support for the system
	SerQ2:IT team has technical competence
	SerQ3:Information system department is responsive, timely and reliable
	SysQ1: Staff utilize the capabilities of an information system
	SysQ2: Appropriate use of the system
	SysQ3: Extensive use of the system
	SysQ4: Staff understand every function of the AIS
	USQ1:Users are satisfied with system report
	USQ2:Users are satisfied with the IT team support
Level of Security Awareness (LOSA)	*LOSAQ1*: You are able to know when your computer is hacked
	LOSAQ2: You know who to contact in case you are hacked or if your computer is infected
	LOSAQ3: You ever found a virus or Trojan on your computer at work
	LOSAQ4: You know what a phishing attack
	LOSAQ5: You know what an email scam is and how to identify one
	LOSAQ6: Is ant-virus currently installed, updated, and enabled on your computer
	LOSQ7: You use the same password for your work accounts as you do for your personal accounts at home, such as Facebook, Twitter, or your email accounts
Demographic Characteristics (DC)	*Age*
	Gender
	LOE: Length of Employment
	NOYWBS: Number of years working
	USAGE. AIS: How long you have used the AIS
Cybersecurity Performance (CP)	AIS easily identify the type of cybercrime/ cyber threat
	AIS determines the nature of cybercrime or cyber risk
	AIS is automated to avoid system hacking
	AIS serves as a security fire wall to prevent cybercrime
	AIS has the capability to signal staff of possible system hacking threat
	AIS sends a notification message to IT security team of possible cybercrime threat
	AIS is able to backup all hacked system data and information
	AIS is automated to restored software/system when hacked

Source*: Author's Construct (2021)*

3.9 PLS-SEM results

As the first step in PLS-SEM, missing data imputation is carried out by Stochastic Multiple Regression Imputation algorithm. The latent constructs consist of reflective measurement scales which are interchangeable and must be highly correlated. In the initial assessment of the model, the loadings of all the variable indicators in the constructs are used for scale purification. Any indicator which has less than 0.5 loadings is dropped from the model. This means that the indicator is different from the rest and must be dropped. From this backdrop, SUQ1, SUQ4, IQ4, SysQ4, CSPRQ3, and CSPRQ4 because they all had a loading of less than 0.5.

3.10 Internal Consistency Reliability assessment

Traditionally, the "Cronbach's alpha "is used to measure internal consistency reliability but it tends to provide a conservative measurement in PLS-SEM. According to Hair et al. (2012), prior literature has suggested the use of composite reliability as a replacement. From this backdrop, the study reported the composite reliability in Table 2. The satisfactory range for composite reliability values is 0.60 to 0.70 in exploratory research and 0.70 to 0.90 in more advanced stages of research. As shown in Table 2, the composite reliability score of all the latent constructs are in the range 0.8188 to 0.9340 indicating that latent variables are reliable.

Table 2: Reliability and validity of latent construct

Measurement Scale and indicators	Standard factor loading			Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted
	Loadings	t-value	P-value				
Effectiveness of AIS (EAIS)				0.9231	0.9282	0.9340	0.6135
SUQ2	0.7359	11.8034	0.0000				
SUQ3	0.7911	12.4529	0.0000				
IQ1	0.7570	12.6735	0.0000				
IQ2	0.6898	9.9273	0.0000				
SerQ1	0.7492	11.6801	0.0000				
SerQ2	0.7034	10.1161	0.0000				
SerQ3	0.7077	10.1161	0.0000				
SysQ1	0.7307	11.2651	0.0000				
SysQ2	0.7380	13.7903	0.0000				
SysQ3	0.7969	13.8902	0.0000				
USQ1	0.8088	10.7417	0.0000				
USQ2	0.5212	4.2835	0.0000				
USQ2	0.6319	5.3887	0.0000				
Level of Awareness (LOA)				0.8706	0.8876	0.9036	0.6135
LOSAQ1	0.8324	14.2164	0.0000				
LOSAQ2	0.5606	5.4196	0.0000				
LOSAQ3	0.7936	11.1653	0.0000				
LOSAQ4	0.8117	12.7093	0.0000				
LOSAQ5	0.8031	14.1307	0.0000				
LOSAQ6	0.8603	15.4040	0.0000				
Demographic Characteristics (DC)				0.7221	0.7773	0.8188	0.5123
Age	0.7968	11.8154	0.0000				
Gender	0.5116	4.0216	0.0000				
LOE	0.5051	4.4831	0.0000				
NOYWBS	0.7867	13.0046	0.0000				
USAGE. AIS	0.8099	12.0250	0.0000				
Cybersecurity Effectiveness (CE)				0.9141	0.9229	0.9275	0.5201
CSPAQ1	0.6064	5.7722	0.0000				
CSPAQ2	0.6610	6.1717	0.0000				
CSPAQ3	0.7763	10.5387	0.0000				
CSPDQ1	0.7118	9.7493	0.0000				
CSPDQ2	0.7958	12.6745	0.0000				
CSPDQ3	0.5149	4.8608	0.0000				
CSPDQ 4	0.8300	10.7747	0.0000				
CSPDet.Q1	0.7205	9.8819	0.0000				
CSPDet.Q2	0.7373	10.3105	0.0000				
CSPDet.Q3	0.7982	10.7700	0.0000				
CSPRQ1	0.7921	10.4131	0.0000				
CSPRQ2	0.6421	5.2965	0.0000				

Since the construct qualify, composite reliability test along with the criteria of average variance extracted (AVE) value is greater than 0.5, the latent variables are retained in the model. Again, Table 2 shows the indicator reliability which is basically the squares of the loading. It can be seen that all the indicators' reliability values are much larger than the minimum acceptable level of 0.4 and close to the preferred level of 0.7.

3.10.1 Convergent validity

According to Wong (2013), it is relevant to check the construct validity of each variable's Average Variance Extracted. If all the AVEs are greater than the threshold of 0.5 the convergent validity is confirmed. From Table 2, all the AVEs are more than 0.5 so the convergent validity is confirmed.

3.10.2. Discriminant validity

Hair et al., (2012) as cited in Kumar and Sujit (2018) argued that discriminant validity certifies that a constructed measure is empirically distinctive and represents facts of interest that other measures in a structural equation model do not capture.

Table 3: Correlation among latent variables with square roots of AVEs

	CE	DC	EAIS	LOA
CE	**0.7212**			
DC	0.8676	**0.6967**		
EAIS	0.9792	0.8719	**0.7239**	
LOA	0.9475	0.7992	0.9283	**0.7833**

Table 3, shows the Fornell–Larcker criterion which suggests that the square root of average variance extracted must be greater than the correlation of the construct with all other constructs in the structural model. Table 3 shows the correlations among latent variables with the square root of average variance extracted (AVE) by each latent variable. It can be seen that each latent variable average variance extracted (AVEs) is higher than the correlation of the latent variables indicating discriminant validity of the latent variables.

3.11 Ethical considerations

The ethical issues that were considered in this study included informed consent, confidentiality, and anonymity. In terms of informed consent, all respondents were appropriately educated on the purpose of this study and then given the chance to decide on participation. Thus, none of the respondents were forced in any way to participate in this study. On the other hand, confidentiality was ensured in the sense that, the responses attained for respondents were solely used for research purposes only. With regards to anonymity, the researcher ensured that the identity of the respondents are safeguarded. In this regard, any information that sought to expose the identity of the respondents such as their name, e-mail address, phone number, and residential address were excluded from the questionnaire.

CHAPTER FOUR

RESULT AND DISCUSSION

4.0 Overview

This study focuses on the results and discussion of the primary data collected for the study. This starts with the demographic and is followed by findings relating to the effectiveness of Accounting Information System usage, level of cybersecurity awareness among staff, and the effect of Accounting Information System on cybersecurity performance. The data was collected from 41 staff in the following commercial banks GCB, Zenith Bank, Republic Bank, and CBG operating in winneba, comprising of 15, 6, 11, and 8 staff respectively.

4.1 Demographic information

The demographic information gathered from the respondents to establish their background were sex, age, the highest level of education, number of working experience in the banking sector, and Accounting Information System usage among staff. These were considered significant because they influence the effectiveness of Accounting Information system/software and the extent of cyber security awareness level among staff and to a greater extend assessing the biasness from the response to the items.

Table 4: Demographic Information (41)

Variable	Frequency(41)	Percentage (%)
Sex		
Male	23	56.1
Female	18	43.9
Age		
21 - 30	14	34.1
31 - 40	22	53.7
41 - 50	5	12.2
Highest Level of Education		
Diploma	1	2.4
HND	4	9.8
First Degree	25	61.0
Masters	8	19.5
Other Qualification	3	7.3
Number of years working in the banking sector		
1 - 5 years	18	43.9
6 - 10 years	18	43.9
11 - 15 years	5	12.2
Usage of Accounting Information System/Software		
Daily	3	7.3
weekdays	38	92.7

Source: Field work, 2021

From Table 4, the result portrays excess male dominance, twenty-three (23) of the respondents representing 56.1% were male whiles eighteen (18) representing 43.9% of the respondents were females. This reveals that most of the views gathered for the analysis were from male staff as compared to that of female staff.

In addition, from table 4, the findings revealed that most of the respondents were between the ages of 21–30. Twenty-two (22) constituting 53.7% indicated that they were between the age range of 21-30; fourteen (14) constituting 34.1% were

between the ages of 31-40, whilst five (5) constituting 12.2% were within the age range of 41-50. From the result, majority of the respondents were between 31 years to 40 years, this indicates that the banks had engaged or employed individuals as its staff in their adult-youth age. This is not surprising because the youth are usually recognized when it comes to knowledge level in Information Communication and Technology (ICT) with software usage.

Also, from Table 4, the findings showed that the respondents had varying educational backgrounds and qualifications. Twenty-five (28) of the respondents representing 61.0% were Bachelor Degree holders, whiles eight (8) representing 19.5% were Master's Degree holders. The rest were four (4) representing 9.8% High National Diploma holders, three (3) representing 7.3% indicated other qualifications. These include the Association of Certified Chartered Accountants (ACCA) and the Institute of Chartered Accountants. This reveals that majority of the staff are Bachelor Degree holders and implies that such sector needs a knowledgeable and educated individual to assist in its daily verities of services rendered to its customers.

Furthermore, it is important to note that since this study also seeks to investigate the level of awareness with regards to cyber-security within the banking sector, the number of years of experience working in the banking sector has to be known. This would give a general idea of how the respondents know possible cyber-security threats to Accounting Information System usage. Also, how long (duration) the respondents have been working with the bank would be necessary since this would enable respondents to effectively interpret their views concerning the effectiveness of Accounting Information System/Software usage and its effect on cyber-security performance. Form Table 4, 43.9% representing eighteen (18) of the respondents have been with their current organisation between 1-5 years, between 6-

10 years, 43.9% representing eighteen (18) of the respondents, and 11-15 years, 12.2% representing five (5) respondents. This shows that the respondents who have worked for a period between 1-5 years and 6-10 years have a piece of fairly sound knowledge on the usage and effectiveness of Accounting Information System/ software of the bank.

Finally, the result from Table 4, indicates that 38 of the respondents representing 92.7% use Accounting Information system (AIS) during the weekdays (working hours) whiles 3 representing 7.3% of the respondents uses Accounting Information system (AIS) daily. This indicates that majority of the respondents use Accounting Information system during the weekdays thus working hours period and would provide the respondents a fair idea concerning the effectiveness of Accounting Information System within the bank's operations.

4.2 Research Objective 1: The effectiveness of Accounting Information System usage.

This section present the results for the first objective of this study which is to examine the effectiveness of Accounting Information System usage. To achieve this objective, the data was analysed into means and standard deviation. The mean scale of 1 to 5 was used where 1= Strongly Disagree; 2 = Disagree; 3 = Neutral; 4 = Agree and 5 = Strongly Agree.

Table 5: Effectiveness of Accounting Information System

		Mean	Mode	Std	Skweness
System Quality	*SQ1*:The system is reliable	4.26	4.00	0.51	0.41
	SQ2: The system easy to learn and understand its features	4.34	4.00	0.59	-0.25
	SQ3: The response time for the system is fast	4.40	4.00	0.50	0.43
	SQ4: The system is flexible	4.23	4.00	0.55	0.12
Information Quality	*IQ1:*Management reports are reliable	4.03	4.00	0.30	0.90
	*IQ2:*Web pages are accurate and upload	4.20	4.00	0.72	-0.82
	IQ3: System output are clear	4.43	5.00	0.78	-1.34
	IQ4: The information from AIS improves the quality of work	3.86	4.00	0.55	-1.22
Service quality	*SerQ1:* IT team provide support for the system	3.66	4.00	0.68	-1.20
	SerQ2:IT team has technical competence	3.69	4.00	0.63	-1.13
	SerQ3:Information system department is responsive, timely and reliable	4.09	4.00	0.28	3.09
System Use	*SysQ1*: Staff utilize the capabilities of an information system	4.51	5.00	0.56	-0.59
	SysQ2: Appropriate use of the system	3.91	4.00	0.75	-0.30
	SysQ3: Extensive use of the system	3.74	4.00	1.07	-0.53
	SysQ4: Staff understand every function of the AIS	3.97	4.00	0.57	-0.01
User Satisfaction	*USQ1*:Users are satisfied with system report	3.86	4.00	0.65	-1.23
	USQ2:Users are satisfied with the IT team support	3.66	4.00	0.94	-0.60
	USQ3: Users are satisfied with AIS interface	3.97	4.00	0.57	-0.01

Source: Fieldwork (2021)

Table 5 above presents the response to the study sample on all the items related to the "Effectiveness of Accounting Information System" measured based on five variables; system quality, information quality, service quality, system use, and user satisfaction. From the table above, it can be observed that the highest mean (arithmetic average) and standard deviation of respondent responses to the item of "system quality" was (M=4.40) and (SD=0.50) for SQ3: "response time for the system is fast" which shows a high level of agreement, this implies that staff response to the construct was in agreement with the scale of 4 and the standard deviation reveals that the response doesn't vary far from the individual response, indicating there is a positive response time with Accounting Information System for their operation, enables to accomplish the task easily and quickly. The lowest mean and standard deviation was (4.23) and (SD=0.55) for SQ4: "System flexibility" which indicates that a high degree of agreement and that staff response to the construct were in agreement with the scale of 4 and the standard deviation reveals that the response doesn't vary far from the individual response. In other words, the Accounting Information System used by the selected commercial banks enables adjustments and other changes to their business operation process. The weighted average mean for the whole dimensions under "System Quality" (SQ) was 4.31, which indicates a high degree of agreement. This implies that the system quality of AIS within the commercial banks is reliable, assist staff to easily complete their task quickly, and enables adjustment and other changes related to their operational process as well as easy to learn and understand AIS features.

In addition to the table above, it can be observed that the highest mean (arithmetic average) with a standard deviation of respondent responses to the item of "Information quality" is (M=4.43) and (SD=0.78) for IQ3: "System output is clear"

which shows a high level of strong agreement, and implies that staff response to the construct was in agreement with the scale of 5 and the standard deviation reveals that the response doesn't vary far from the individual response, indicating that the information generated by the system provides clear understanding information to management for better management decision and planning. The lowest mean and standard deviation was (M=3.86) and (SD=0.55) respectively for IQ4: "the information from AIS improves the quality of work" which indicates that a high degree of agreement, this implies that staff response to the construct was in agreement with the scale of 4 and the standard deviation reveals that the response doesn't vary far from the individual response. In other words, AIS used by the selected commercial banks increases the rate of quality work via their daily transactional activities rendered to their customers and as well as for better matter management planning and decision making. The weighted average mean for the whole dimensions under "Information Quality" (IQ) was 4.13, which proves a high degree of agreement. These responses imply that the processed data into information by AIS results in providing management with a reliable and accurate report at any point in time with understandable information that improves the quality of service rendered to their customers as well as aided management to make an informed decision.

Also, from table 5 above, it can be observed that the highest mean with a standard deviation of respondent responses to the item of "Service Quality" was (M=4.09) and (SD=0.28) for SerQ3: "Information system department is responsive, timely and reliable" which shows a high level of strong approval and this implies that staff response to the construct was in agreement with the scale of 4 and the standard deviation reveals that the response doesn't vary far from the individual response. This implies that there is an information system department within the selected banks that

provides timely responses to any related issues with the Accounting Information System by way of providing reliable solutions to enable staff to perform effective transactional operations. The lowest mean with a standard deviation was (M=3.66) and (SD=0.68) respectively for SerQ1: "IT team provide support for the system" which indicates that a high degree of agreement and implies that staff response to the construct was in agreement with the scale of 4 and the standard deviation reveals that the response doesn't vary far from the individual response. In other words, the IT team that works within the banks provides the necessary support service to staff members when the need arises concerning Accounting Information system issues. The weighted average mean response to the whole questions under "Service Quality" (SerQ) was 3.81, which proves a high degree of agreement. These responses imply that there is competent and experience IT team within the information system department of these selected banks that provide the required service support to its colleagues within the institutions to process data into information that results in providing management with reliable and accurate up to date information at any point in time.

Moreover, from table 5 above, it can be observed that the highest mean with a standard deviation of respondent responses to the item of "System Use" was (M=4.51) and (SD=0.56) respectively for SysQ1: "Staff utilizes the capabilities of an information system" which shows a high level of strong approval, this implies that staff response to the construct was in agreement with the scale of 5 and the standard deviation reveals that the response doesn't vary far from the individual response, indicating that staff member can utilize the capabilities of AIS effectively to the benefit of the organisation in terms of satisfying its customers. The lowest mean with a standard deviation was (M=3.74) and (SD=1.07) respectively for SysQ3: "Extensive

use of the system" which indicates that a high degree of agreement and that the response from respondents does not vary from the individual response. In other words, staff are able to extensively put AIS into good utilization during its transactional operations in line with rendering service to customers and providing service to management. The weighted average mean response to the whole construct under "System use" (SysQ) was 4.03, which indicates a high degree of agreement. These responses implies that staff understands every function of AIS used within the bank and proves to appropriately put AIS into extensively good utilization to improve effectiveness within the organisation.

Finally, from table 5 above, it can be observed that the highest mean with a standard deviation of respondent responses to the item "User satisfaction" was (M=3.97) and (SD=0.57) respectively for USQ4: "Users are satisfied with AIS interface" which shows a high level of strong agreement with the scale of 4, and the standard deviation reveals that the response doesn't vary far from the individual response, indicating that staff is really satisfied with inbuilt interface of AIS used within the organisation and makes their work easy by operating the system/software with any difficulty. The lowest mean with a standard deviation was (M=3.66) and (SD=0.94) respectively for USQ2: "Users are satisfied with IT team support" which indicates that a high degree of agreement with the scale of 4 and that the response from respondents does not vary from the individual response. In other words, the staff is satisfied with IT support services provided for the system in line with their usage. The weighted average mean response to the whole construct under "User satisfaction" (USQ) was 3.83, with a scale of 4 for each construct. This indicates a high degree of agreement. These responses implies that staff is satisfied with IT team support services provided to the system, with the interface developed unto the system which

enables their operationalization of AIS easy with no difficulty, and also satisfied with the report generated by the software for decision making.

4.3 Research Objective 2: The level of awareness of Cyber Security among the staff of universal banks.

This section present the results for the second objective of this study which is to assess the level of awareness of Cybersecurity among staff on universal banks. To achieve this objective, the data was analysed into means and standard deviation. The mean scale of 1 to 5 was used where 1= Strongly Disagree; 2 = Disagree; 3 = Neutral; 4 = Agree and 5 = Strongly Agree.

Table 6: The level of awareness of Cyber Security among the staff of universal banks

	Mean	Mode	Std	Skewness
LOSAQ1: You are able to know when your computer is hacked	3.69	4.00	0.72	-1.46
LOSAQ2: You know who to contact in case you are hacked or if your computer is infected	3.00	4.00	1.06	-0.79
LOSAQ3: You ever found a virus or Trojan on your computer at work	3.09	4.00	0.98	-0.77
LOSAQ4: You know what a phishing attack	1.23	1.00	0.43	1.35
LOSAQ5: You know what an email scam is and how to identify one	3.97	4.00	0.30	-0.90
LOSAQ6: Is ant-virus currently installed, updated, and enabled on your computer	3.49	4.00	4.00	0.82
LOSQ7: You use the same password for your work accounts as you do for your personal accounts at home, such as Facebook, Twitter, or your personal email accounts	3.00	4.00	4.00	1.34

Source: Fieldwork (2021)

Table 6 above presents descriptive data on the level of awareness of Cybersecurity among staff. From the table above, it can be observed that the mean

values of the response to the questions on the level of cybersecurity awareness among staff are between 1.20 and 3.98, this shows that responses from respondents which are agree and strongly agree were more than that of disagree or strongly disagree. On whether staff can know when their computer is hacked, the respondent agreed (M=3.69). Respondents also agreed that they know who to contact in case their computer system is hacked or when their computer is infected with a virus (M=3.00) in addition to asserting whether staff had ever found a virus or Trojan on their computer at work, respondents agreed (M=3.09). Also, respondents posit that they know what an e-mail scam is and how to identify one (M=3.97).

Again, respondents agreed that antivirus is installed, updated, and enabled on their computer (M=3.49). Moreover, respondents agreed that they use the same password for their office system account as they do for their personal accounts at home such as Facebook, Twitter, and or their personal email account (M=3.00). Despite the responses from staff of the selected universal banks, a significant number of them consented that, they strongly disagree that they know phishing attacks (M=1.23). Therefore, according to the respondents' reply is possible to conclude that most respondents had a fair level of knowledge on cybersecurity-related issues.

4.4 Research Objective 3: The effect of Accounting Information System effectiveness on Cybersecurity performance.

This section present the result for the last objective of this study which is to investigate the effects of Accounting Information System on cybersecurity performance. To achieve this objective the Smart PLS results were used to determine the effect on cybersecurity performance by variables (AIS effectiveness, demographic

characteristics and level of security awareness) that is displayed in Figure 3 and Table 7.

Table 7: Structural Path Significance in Bootstrapping

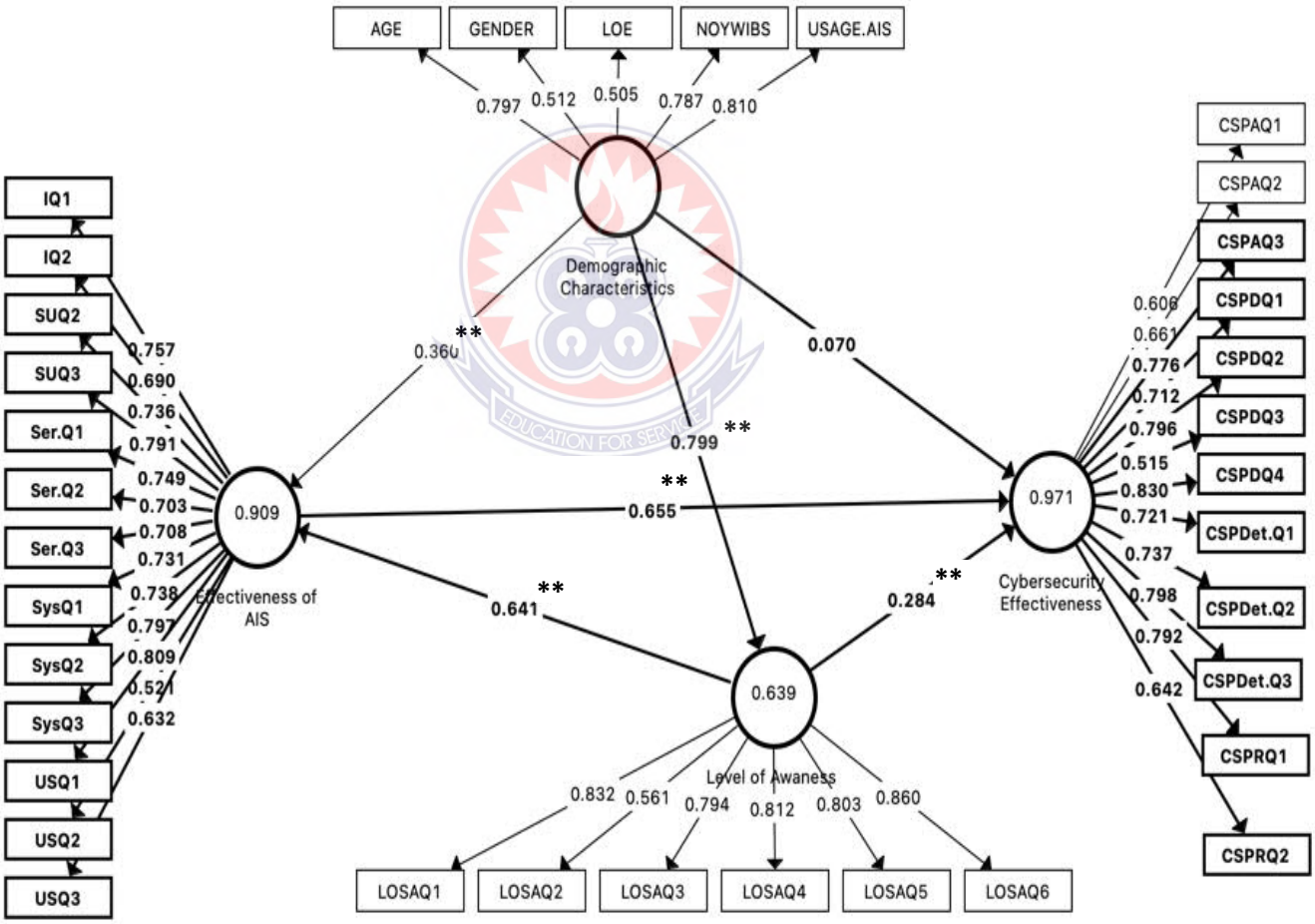
	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
Demographic Characteristic ->Cybersecurity Performance	0.0698	0.0793	0.0475	1.4696	0.1423
Demographic Characteristic ->Effectiveness of AIS	0.3598	0.3675	0.0785	4.5835	0.0000
Demographic Characteristic ->Level of Awareness	0.7992	0.8054	0.0440	18.1554	0.0000
Effectiveness of AIS ->Cybersecurity Performance	0.6549	0.6373	0.0852	7.6873	0.0000
Level of Awareness ->Cybersecurity Performance	0.2837	0.2934	0.0679	4.1779	0.0000
Level of Awareness -> Effectiveness of AIS	0.6407	0.6336	0.0759	8.4448	0.0000

Source: Field work (2021)

The result indicates that the coefficient of determination, R^2 is 0.971 for endogenous latent variables. This means that, the variables (Demographic characteristics, Effectiveness of Accounting Information System, and Level of security awareness jointly explained 97.1% of the variance of the overall cybersecurity performance. The Smart PLS result also indicates the variables sequentially had path coefficient as follows; are 0.0698 for the effect of Demographic characteristics, 0.6549 for the effect of Effectiveness of Accounting Information

System, and 0.2839 for the effect of Level of cyber security awareness. This implies that the Effectiveness of AIS has the strongest effect on cybersecurity performance.

Also, Table 7 displays structural path significance in bootstrapping, the outcomes of the effect of demographic characteristics on cybersecurity performance [t=1.4696, P<0.005], the effectiveness of Accounting Information System (AIS) on cybersecurity performance [t=7.6873, P<0.05], and level of security awareness on cybersecurity performance [t=4.1779, P<0.05] were all statistically significant at 5%. The results indicate the direct effect of the variables on cybersecurity performance.



**Indicates significant at 5% level of significance i.e. $p = <0.05$.

Figure 3: Path Diagram model of the effect of AIS effectiveness on Cybersecurity Performance

Source: Field Study (2021)

4.5 Discussion

The study was driven by the increasing rate of banking fraud and cybercrime activities that affects the banking operations in the central of Ghana and the world as a whole. The study seeks to delve to assess the effectiveness of Accounting Information System, the level of cybersecurity awareness among staff, and cybersecurity performance among the selected banks in the central region precisely Winneba in Effutu Municipality. This section provides an in-depth discussion on the results presented in chapter four. The discussion begins with the demographic characteristics of respondents before the three objectives of the study are discussed in detail.

4.5.1 Demographic Information

Anwar et al. (2017) noted socio-demographic characteristics have also been found to have a moderating effect on the cybersecurity behaviors of employees. These variables include gender, age, marital status, religion, ethnicity, employment status, and level of education but for this study, because the population of the respondents were staff working within the banking sector, the demographic characteristics used for the study included sex, age, level of education, number of years working within the banking sector and how often a staff uses Accounting Information System. Furthermore, in a study that investigated the familiarity of employees with an undergraduate certificate with cyber threats, it was found out that the employees were less familiar with cyber threats (Jeske & Van Schaik, 2017). It is, therefore, imperious to analyse these socio-demographic characteristics of the respondents to ascertain their practical significance for the study.

4.5.1.1 Sex of Respondents

The result showed that most of the respondents (56.1%) were male, which implies that most of the responses from this study are male prejudice and it was expected because of the less number of dominated males as compared to that of females within banking institutions. This finding is consistent with the findings of Ogutcu and Chouseinoglon (2016) that studies conducted within the technological institution are likely to have a marginal increase in the percentage of males dominating managerial roles using Accounting Information System compared to females.

4.5.1.2 Age of Respondent

Whitty et al. (2015), found that younger people were significantly more likely to engage in the poor security practice of password sharing. Venkatesh, Morris, & Davis (2013) found that age is an important demographic predictor in organizations. To this, the prior research states that increasing age has lower attitudes towards its usage, and acceptance behavior (Igbaria et al. 2011). The reasoning for this could be that older people have less computer experience, are less open to change, and relatively are not good at managing computer-related documents. From the result, majority of the respondents (53.7%) were between the ages of 31 to 40 years, followed by 14.34% between 21-30 years and 12.2% between 41-50 years. This implies that the findings of the study are based on the youth because the findings reflect the opinions of the youth who are the most active population in the banking sector. This will also go a long way to assist management to draft a policy to protect the interest of the youth and train them to maintain them towards effective and efficient operationalization of Accounting Information software in serving their clients.

4.5.1.3 Level of education

From Table 4, first degree holders dominated the level of education of the respondents representing 61.0%, Master's degree holders represented 19.5%, HND holders represented 9.8%, other qualifications representing 7.3%, and Diploma holders 2.4%. This finding is significant in the sense that the level of one's education affects the usage, understanding, and implementation of Accounting Information System. In addition, it is expected that if staff members have a reasonable level of education this is likely to influence the usage and implementation of computerized accounting systems. These findings are consistent with the results of Amidu, Effah & Abor (2011) on e-accounting practices and SMEs in Ghana, which showed that most of the employees sampled had higher levels of education such as diplomas, degrees, and professional qualifications.

4.5.1.4 Number of years working in the banking sector

From Table 4, 1-5 years and 6-10 years equally dominated the period of working experience within the banking sector of respondents representing 43.9% and 43.9% respectively and 11-15 years representing 12.2%. Someone who performs the same task repeatedly will keep more things in his memory and can develop a good understanding of the various events of Ariani (2010). Work experience is the period or length of time someone works in an agency, office). The more experience a person has in his field of science, the easier it will be for him to learn new things to improve his performance, this is in line with the research of Ariani (2010) and Adrian (2015) stating the influence of experience has a positive effect on AIS effectiveness Skill is an ability, talent or skill that exists within every human being Adrian (2015). From this backdrop, because most of the respondents had worked for some period of years,

plays a major role to improve the effectiveness of AIS since the staff is mostly used to operating the software.

4.5.2 Research Objective 1: Examine the effectiveness of Accounting Information System Usage

The first objective of the study seeks to examine the effectiveness of Accounting Information System within selected universal banks in winneba (GCB, Zenith Bank, Republic Bank, and CBG). Overall, the findings of the study revealed that majority of the respondents asserted and agreed that for Accounting Information System to function effectively it should possess some information system characteristics which include system quality, information quality, service quality, friendly system use, and user satisfaction. It revealed through the study that majority of the respondents accepted that AIS used by the universal banks is of system quality since majority of staff members agreed that the system is reliable, easy to learn and understand its features, able to provide timely response and system flexibility which easily assist staff to complete their task quickly, and enables adjustment and other changes related to their operational process in line with rendering services to their customers and clients. As far as information quality is of concern to AIS effectiveness, the study found out that respondents asserted that AIS provides quality information, that's majority of the respondents agreed that AIS provides management reliable report, output information is clear and understandable as well as the information has enabled staff members to improve their quality of the information provided to their clients.

The study also revealed that majority of the respondents agreed that the IT team has the technical competence to provide support for the system which directly indicates that there is service quality of AIS operated by the selected universal banks.

Concerning system use and user satisfaction, it was revealed that majority of the respondents strongly agreed staff utilize the capabilities of the system, understands every function of AIS, satisfied with the interface developed unto the system which enables their operationalization of AIS easy with no difficulty and also satisfied with the report generated by the software for decision making. This confirms the findings of Al-Hantawi, (2010) who indicated that the most important characteristics that qualify accounting information systems as effective and efficient are the system quality, user satisfaction, service quality, information quality, and speed of processing financial data into accounting information, therefore providing management with the necessary accounting information on time; providing management with the necessary information to perform functions of planning, control, evaluation, speed and accuracy in retrieving stored overall and descriptive information when it is needed; adequate flexibility; general acceptance of workers; simplicity, and to be associated with other information systems in the entity.

4.5.3 Research Objective 2: assess the level of awareness of cyber security among staff

The second objective of the study sought to assess the level of cyber security among staff in the selected universal banks in Winneba. Overall, the findings of the study revealed the following; about staff knowing when their computer is hacked, knowing who to contact when there are cybercrime-related issues, able to identify a computer virus or Trojan the operating Accounting Information System, knowledgeable and informed about related cyber security issues, the study found out that majority of the respondent agreed that they have a high level of knowledge concerning Accounting Information System issues and possible online related system crime and hacking. Furthermore, in respect of level of security awareness concerning

whether staff members use the same password for their office software account is similar to that of the password used for their personal account at home, such as Facebook, Twitter, and possibly e-mail account, the study found that majority of the respondent strongly disagreed which indicates how knowledgeable the respondent is aware of the risk involved in using a similar password for several system or application log-in request. Nevertheless, few respondents hold the view that their awareness level is in line with a phishing attack, the study revealed that majority of the respondent strongly disagree that the knows phishing attack and related issues indicating that most of the respondents had a fair level of knowledge on cybersecurity and cybercrime-related issues.

Therefore, this is consistent with the findings of Pramod & Raman (2014) indicating that employees within an organisation are not ignorant of security concerns regarding software applications, but at the same time are fully aware of all the security risks and necessary security practices.

4.5.4 Research Objective 3: determine the impact of Accounting Information System on cybersecurity performance

The third objective of the study sought to determine the impact of Accounting Information System on cybersecurity performance among the selected universal bank under study. A study according to Said and Noha (2019) found that system security performance can be measured based on four components; analyze, defend, detect, and revival. These four components were considered in assessing cybersecurity performance within the selected universal banks in Winneba. The findings of the study revealed that in term of the ability of the system to analyze any form of security threat, majority of the respondents asserted and agreed that the system easily identifies the type of cybercrime/cyber threat, the nature of the cybercrime, and also

provides details on all possible unauthorized system login. It revealed through the study that majority of the respondents accepted that AIS is automated to avoid system hacking, serves as a security firewall to prevent cybercrime, and is also programmed to avoid financial data lost in terms it capacity to defend against cyber threats. As far as the detection capability of the system was assessed the findings revealed that the system had the capability to signal staff of possible system hacking, easily identifies data or information that has been hacked, and also sends a notification message to the IT team of possible cybercrime threat.

Moreover, the findings indicated that majority of the respondents agreed that documents are easily retrieved and restored as well as system backup is easily done to all hacked data and information. The overall findings in assessing the effect of Accounting Information System effectiveness on cybersecurity the study revealed that there is a significant statistical impact on the performance of cybersecurity within the selected during their operations. Furthermore, the results also indicated that both demographic characteristics and level of security awareness of staff members also had a significant effect on the performance of cyber security capabilities. Studies carried by Gordon, Loeb, Lucyshyn, and Sohail (2006) highlighted the impact of cybercrime reduction of information-security threat activities by corporations. They clearly emphasized that management's decision to implement an effective and efficient Accounting Information System had a positive impact on such threat reduction. Therefore, having effective Accounting Information System is a foundation for cybersecurity performance within organisation.

CHAPTER FIVE

SUMMARY, CONCLUSION, RECOMMENDATION AND SUGGESTIONS FOR FURTHER STUDIES

5.1 Overview

This study investigated the effect of Accounting Information System effectiveness and firms Cybersecurity performance among selected universal banks in Winneba (GCB, Zenith Bank, Republic Bank, and CBG). This was done with a sample of 41 through the census sampling techniques. The questionnaire with Cronbach alpha range 0.8188 to 0.9340 was used as a research instrument to collect data. The study employed an interview schedule and the quantitative data was analysed using Statistical Package for Social Sciences (SPSS) version 25.0 software and Smart PLS. in this chapter, the summary of the study, conclusion, recommendations, and suggestions for further studies are also presented.

5.2 Summary of the findings

5.2.1 Effectiveness of Accounting Information System

In relation to the first objective which examines the effectiveness of Accounting Information System, it was found that majority of the respondent (staff) asserted and agreed that for Accounting Information System to function effectively it should possess the following information system characteristics which include system quality, information quality, service quality, friendly system use, and user satisfaction. The study revealed that staff utilize the capabilities of the system, understands every function of AIS, satisfied with the interface developed unto the system which enables their operationalization of AIS easy with no difficulty and also satisfied with the report generated by the software for decision making. This confirms the findings of

Al-Hantawi, (2010) who indicated that the most important characteristics that qualify accounting information systems as effective and efficient are the system quality, user satisfaction, service quality, information quality, and speed of processing financial data into accounting information, therefore providing management with the necessary accounting information on time; providing management with the necessary information to perform functions of planning, control, evaluation, speed and accuracy in retrieving stored overall and descriptive information when needed.

5.2.2 Level of awareness of Cyber Security among the staff of universal banks

The findings on the second objective which investigated the level of awareness among staff about cybersecurity, the study revealed that the respondents agreed to the fact that they had a fair knowledge on ability to dictate when their computer is hacked, e-mail scam and easily knows who to contact when cybercrime issues arise during the period of operating the application software. Moreover, the study reveals how knowledgeable staff (employees) are in terms of risk involved in using a similar password for several system or application log-in request. Nevertheless, few respondents hold the view that they have low awareness level in line with a phishing attack cybercrime related issues.

5.2.3 Impact of Accounting Information System on Cybersecurity performance

Findings from the third objective which investigated the effect of Accounting Information System effectiveness on cybersecurity performance showed, that there is a significant statistical effect of the effectiveness of Accounting Information System to impact the firm's cybersecurity performance in terms of its capability to analyze, defend, detect, and retrieve hacked data or information. Also, it was revealed that

demographic characteristics and level of security awareness of staff had an impact on cybersecurity.

5.3 Conclusion

It can be concluded that the Accounting Information System used by the select universal banks has proven to be effective by the respondents (staff) response because the Accounting Information System/Software used by the banks possess some required information system characteristics namely; system quality, information quality, service quality, system use, and user satisfaction which directing influences their daily operational transactions rendered to their customers and clients. In addition, the level of knowledge base issues in relation to information security or cybersecurity, staff members had fair knowledge on the ability to dictate when their system is hacked, online scam email messages and knows who they ought to contact when cybersecurity-related issues occur when using the computer application software. On the other issue of the effect of Accounting Information System effectiveness on cybersecurity performance, it is concluded that the information system characteristics (System quality, information quality, service quality, system use, and user satisfaction) has an influence the on firms capability to reduce or eliminate all forms any cybercrime and cyber threat. Nevertheless, demographic characteristics and level of security awareness of staff (employees) can equally influence the banks' performance in respect of cybersecurity. Concerning the effect of Accounting Information System effectiveness on cybersecurity performance, the study concludes that the ability of firms to acquire computer application system or software that possess the required information system characteristics and individuals (staff) has a fair knowledge and understanding of cybercrime-related issues has a

great impact on reducing and preventing firms (banks) from any cyber threat or cybercrime.

5.4 Recommendations

In the light of the findings and conclusions of this study, the following recommendations are put forward:

i. It has emerged that the Accounting Information System utilized by the selected banks possesses some information system characteristics that enable the institutions to effectively render the necessary services needed to their customers. In this regard, management of these banks should make sure such information system characteristic is maintained and possibly system update are done when necessary.

ii. The study also found that staff had a fair knowledge on security-related issues precisely cybercrime or cyber threat and management should take online and system threats as a priority and constantly educate and organise training for its staff on cybersecurity-related matters to broaden the knowledge scope of its employees.

iii. The findings of the study indicated that Accounting Information System with information system characteristics (system quality, information quality, service quality, system, and user satisfaction) as well as demographic characteristics and level of security awareness of staff has the influence to affect the performance of the firms in relation to cybersecurity. From this backdrop, management should make sure that Accounting Information System loses not its effectiveness but rather try to improve on its effectiveness, increase the knowledge base of its staff and

also take into consideration the demographic characteristics when seeking new staff.

5.5 Suggestions for further studies

The study focused on the effectiveness of Accounting Information System and cybersecurity performance of selected universal banks in Winneba. It is suggested that a large-scale study be conducted on the effectiveness and efficiency of Accounting Information System on cybersecurity performance from both public and private financial institutions in Ghana to expand coverage of the study to draw a valid conclusion.

REFERENCES

Adeyinka, O. (2008). Internet Attack Methods and Internet Security Technology: Modeling & Simulation, 2008.AICMS 08. *Second Asia International Conference,* 77-82, 13-15.

Adrian, (2015). *Effect of Position, Age, Experience, Level of Education and Skill on the Effectiveness of Accounting Information Systems at PT. PLN (Persero) South Bali Area.* Encryption, Mahasaraswati University.

Agbim CP, (2013).*The effects of computerized accounting system on the performance of banking industry in Nigeria.* Nigeria: Caritas University.

Al-Hantawi, M. Y. (2010). *Accounting information systems.* Amman, Jordan: Wa'el Press for Publication and Distribution.

Al-Helo, B. S. (2015). Impact of using information technology and systems on integrated banking services in Jordanian banks from the perspective of banking leaderships, (unpublished Master thesis) Al Al-Bayt University, Mafraq, Jordan.

Alia, A., Rahman, M.S.A., & Ismail, W. (2012). Predicting continuance intention to use accounting information systems among SMEs in Terengganu, Malaysia. *International Journal of Economics and Management, 6*(2), 295-311.

Al-Omiri, M., & Drury, C. (2007). A survey of factors influencing the choice of product coating system in U.K organization. U.*K Article in Management Accounting Research, 18*(4), 399-424.

Amidu, M. (2011). "E-Accounting Practices among Small and Medium Enterprises in Ghana", *Journal of Management Policy and Practice,* vol. 12, no.4, p. 152.

Amidu, M., Effah, J. & Abor, J. (2011), E-Accounting Practices among Small and Medium Enterprises in Ghana. *Journal of Management Policy and Practice,12*(4).

Anwar M, Ash I, Yuan X, Li L, Xu L. (2017),Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 6*(9), 437-43.

Ariani, NN.A., 2010. *Effects of Gender, Position, Age, Experience, Complexity, Tasks and Level of Education on the Effectiveness of Accounting Information Systems at PT.* Flamboyan Creations in Denpasar. Thesis, Warmadewa University.

Banker, R., & Feng, C. (2019). The impact of information security breach incidents on CIO turnover. *Journal of Information Systems 33*(3), 309–329.

Basel, J. A., Baker, R., & Omar, W. A. (2016). The critical success factor of accounting information systems and its impact on organizational performance

of Jordanian commercial banks. *International Journal of Economic, Commerce, and Management, 4*(4), 658-676.

Beke, J. (2010). Review of international accounting and information systems. *Journal of Accounting and Taxation, 2*(2). 139-161.

Bentler, P. M., & Huang, W. (2014). On components, latent variables, PLS and simple methods: Reactions to ridgon's rethinking of PLS. *Long Range Planning,* 47(3), 138–154.

Bently, Y., Cao, G., & Lehaney, B. (2013). The application of critical systems thinking to enhance the effective-ness of a university information system. *System Practice Action Research,* 26, 451-465.

Bisbe, J., & Malague. o, R. (2015). How control systems influence product innovation process: The role of entrepreneurial orientation. *Accounting and Business Research*, *45*(3) 356-386.

Boame, I. Solace. K. and Issaka. S. (2014). Adoption of accounting practices and its effects on SMEs; Financial perspective of sachet water producers in Northern Region of Ghana. *Research Journal of financial and Accounting, 5*(17). 166-179.

Bonollo, E., Lazzine, S., & Merli, M.Z. (2015). Innovation in accounting information systems in public sector. Evidence from Italian public universities. Lecture Notes in Information Systems and Organisation, 199-216. Retrieved from: *https://doi.org/10.1007/978-3-319-26488-2_15*

Bose, R. and Luo, X. (2014). Investigating security investment impact on firm performance. *International Journal of Accounting and Information Management, 22*(3), 194-208.

Butler, R., & Butler, M. (2014). An assessment of the human factors affecting the password performance of South African online consumers. In N. Clarke, & S. Furnell (Eds), *Proceedings of the Eighth International Symposium on Human Aspects of Information Security and Assurance (HAISA 2014)* (pp. 150-160), Plymouth, UK, 8-9 July.

Carbon, B. (2020). *Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks.* Finance Industry Heavily Targeted.

Carr, N. (2013). IT doesn't matter. *Harvard Business Review 81*(5), 41-49.

Cheng, X., & Walton, S. (2019). Do nonprofessional investors care about how and when data breaches are disclosed? *Journal of Information Systems, 33*(3), 163–182.

Chenhall, R. H., & Morris, D. (1986). The impact of structure, environment, and interdependence on the perceived usefulness of management accounting systems. *The Accounting Review.*

Choe, (1998). The effect of user participation of the design of accounting information system. *International Journal of Accounting and Information Management, 22*(3), 194-208.

Chong, P. (1996) Accounting information system as an aid of decision making in Food and Beverage companies in Nigeria. *Australia Journal of Business Management Research,* 3, 26-33.

Cole, K., Chetty, M., LaRosa, C., Rietta, F., Schmitt, D. K., Goodman, S. E., & Atlanta, G. A. (2008). *Cybersecurity in Africa: An assessment. Atlanta, Georgia, Sam Nunn School of International Affairs,* Georgia Institute of Technology.

Dalci, İ., & Taniş, V. N. (2004). Benefits of computerized accounting information systems on the JIT production systems. *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 13*(1).

Dameri, R., Garelli, R., & Ricciardi, F. (2013). The didactic challenge of accounting information systems and ERPs for business schools: A proposal for the Italian universities. *Lecture Notes in Information Systems and Organisation,* 337-349. Retrieved from: *https://doi.org/10.1007/978-3-642-35761-9_21*

DHS. (2014). A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. Retrieved from: *http://niccs.us-cert.gov/glossary#letter_c*

Drigă, I., & Isac, C. (2014). E-banking services–features, challenges and benefits. *Annals of the University of Petroşani, Economics, 14*(1), 41-50.

Easterby-Smith, M. (1991). *Management research: An introduction.* London: Sage Publications.

Elpez, I., & Fink, D. (2010). Information systems success in the public sector: Stakeholders' perspectives and emerging alignment model. *Issues in Informing Science and Information Technology, 3*(2), 219-231.

Erna, (2015). *Effect of Incentives, Education Level, Age, Position, and Employee Work Experience on Individual Performance of Auntansi Information System Users at PT.* Darum Lestari Dinar. (Thesis) Mahasaraswati University.

Fengyi, L., Olivia, R. L., & Sheng, S. W. (2010). An integrated framework for e-chain bank accounting systems. *Industrial Management & Data Systems, 105*(3), 291-306.

Financial Action Task Force (2020). Covid-19-related money laundering and terrorist financing risks and policy responses. *International Journal of Accounting and Information Management, 22*(3), 194-208.

Fontinelle. (2013,). Introduction to Accounting Information Systems. Retrieved from: *http://www.investopedia.com/articles/professionaleducation/11/accounting-information-systems.asp*

Frank, M., Grenier, J., & Pyzoha, J. (2019). How prior cyberattacks influence the efficacy of cybersecurity risk management reporting and independent assurance. *Journal of Information Systems 33*(3), 183–200.

Furnell, S., Gennatou, M., & Dowland, P. (2002). A prototype tool for information security awareness and training. *Logistics Information Management, 15*(5/6), 352-357.

Gelinas, U. J, Sutton, S. G., & Hunton, J. E. (2005). *Accounting information systems, (6th ed.).* Thomson, OH, USA: South-Western.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly,34*(3), 567-594.

Gordon, L. A., Loeb, M.P., Lucyshyn, W., & Zhou, L. (2015b). Externalities and the magnitude of cybersecurity underinvestment by private sector firms: a modification of the Gordon-Loeb model. *Journal of Information Security, 6*(1), 24-30.

Gordon, L., Loeb, M., & Lucyshyn, W. (2015). *The annual CSI/FBI computer crime and security survey, in: CSI (Ed.),* pp 26.

Gordon, L.A. & Loeb, M.P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (Security),* 5(4), 438-457.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Sohail, T. (2006), "The impact of the Sarbanes-Oxley act on the corporate disclosures of information security activities", *Journal of Accounting and Public Policy, 25*(5), 503-530.

Gorla, N., Somers, T. M., & Wong, B. (2010). Organizational impact of system quality, information quality, and service quality. *The Journal of Strategic Information Systems, 19*(3), 207-228.

Grabski, S. V., & Marsh, R. J. (1994). Integrating accounting and manufacturing information systems: An ABC and REA-based approach. *Journal of Information Systems, 8*(2), 61-80.

Greenfield, T. (2016). *Research methods for postgraduates, (3rd ed.).* UK: John Wiley & Sons, Ltd.

Gregory, R. J. (2000). *Psychological testing, history, principles, and applications, (3rd edition).* Boston: Allyn and Bacon.

Gyun No, W., & Vasarhelyi, M.A. (2017). Cybersecurity and continuous assurance. *Journal of Emerging Technologies in Accounting, 14*(1), 1-12.

Hair, J. F., Sarstedt, M., Pieper, T., Ringle, C. M., & Mena, J. A. (2012). The use of partial least squares structural equation modelling in strategic management research: A review of past practices and recommendations for future applications. *Long Range Planning, 45*(5–6), 320–340.

Hair, J., Sarstedt, M., Ringle, C., & Mena, J. (2012). An assessment of the use of partial least squares structural equation modelling in marketing research. *Journal of the Academy of Marketing,* 40, 414 -433.

Halder, D., Jaishankar, K., & Jaishankar, K. (2012). *Cybercrime and the victimization of women: laws, rights and regulations.* Hershey, PA: Information Science Reference.

Hall, J. A. (2010). *Accounting information systems.* South Western Educational Publishing.

Hamed, T. (2016). Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. *International Journal of Academic Research in Management (IJARM)*, *10*(3).

Hien, L. T., Nguyen, T. L., & Cuong, P. H. (2014). Key determinants of information system effectiveness – An empirical case in Lac Hong University. *International Journal of Information Technology and Business Management, 32*(1), 1-14.

Hunton, J. E. (2002). Blending information and communication technology with accounting research. *Accounting Horizons, 16*(1), 55-67.

Igbaria, M., Zinatelli, N., Cragg, P., & Cavaye, A. L. (1997)Personal computing acceptance factors in small firms: a structural equation model. *MISQ.* 21, 279–305.

James H. M., & Schumacher, S. (2006). *Research in education: Evidence Based Inquiry, (6th edition).* England: Pearson Education Limited.

Jeske D, & van Schaik P. (2017). Familiarity with Internet threats: Beyond awareness. *Computers & Security, 6*(6), 129-41.

Kanungo, S., Duda, S., & Srinivas, Y. (2010). A structured model for evaluating information systems effective-ness. *Systems Research and Behavioral Science, 16*(6), 495.

Karanja, E., & Zaveri, J. (2014). Ramifications of the Sarbanes Oxley (SOX) Act on IT governance. *International Journal of Accounting and Information Management, 20*(2), 134-145.

Kaufmann, A. (1966) *Graphs, dynamics programming, sequential management.* London: Sage Publication.

Kaur, J., & Mustafa, N. (2013). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. In IEEE (Ed.), *2013 International Conference on Research and Innovation in Information Systems* (ICRIIS) (286- 290).

Kumar, B. R., & Sujit, K. S. (2018). Determinants of dividends among Indian firms - An empirical study. *Cogent Economics & Finance, 6*(1), 142-389.

Lalin, H., & Sabir, R. I. (2010). Research on Usage and Usefulness Perception of Financial Accounting Practices in Less Developing Countries: A case of Cambodia. *Proceedings of the Proceedings of the 7th International Conference on Innovation & Management,* 1881-1885.

Li, H., No, W., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems,* 30, 40-55.

Mason, E. D., Williams, S., Grotendorst, G. R., Marsh, J. L. (1997). Information and communication technology with accounting research. *Accounting Horizons, 16*(1), 55-67.

McDowall, T., & Jackling, B. (2006), "The impact of computer-assisted learning on academic grades: an assessment of students' perceptions", *Accounting Education: An International Journal,* 15(4), 377-389.

Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Academy of Information & Management Sciences Journal, 14*(2), 91-153.

Merriam-Webster Dictionary (MW). (2020). Cyber-security. Retrieved from: *https://www.merriam-webster.com/dictionary/cybersecurity*

Messick, S. (1989). Meaning and values in test validation. *The Science and Ethics of Assessment, 18*(2), 5-11.

Mishra, U. (2014). Retrieved from: https://Is.*anti.virus.a.necessary.evil.,* on July 6, 2021.

Mugenda & Mugenda, (1999). *Research methods: Qualitative and quantitative approach, research methods in social sciences, (5th edition).* New York: St. Martin's.

Nichols, D., & Holmes, S. (1998). Analysis of the use of accounting information by Australian Small Business. *Australia Journal of small Business Management*

Nicolau, A. S. (2016). Organizational performance effects of ERP systems usage: The impact of post implementation change. *International Journal of Accounting Information Systems.*

Nicolau, A.L. (2000). A contingency model of perceived effectiveness. *International Journal of Accounting Information System, 1*(2), 91-105.

Nitzl, C. (2016). The use of partial least squares structural equation modelling (PLS-SEM) in management accounting research: Directions for future theory development. *Journal of Accounting Literature,* 37, 19–35.

OECD (2012). *OECD Internet Economy Outlook 2012,* OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264086463-en.

Ofanson E. J., Aigbokhaevbolo O. M., & Enubulu G. O. (2010). The financial system in Nigeria: An overview of banking sector reforms. *AAU JMS*, 1.

Ogutcu G, Tastik OM, & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security,* 5(6), 83-93.

Okello-Obura, C. (2009). Business information systems design for Uganda's economic development: the case of SMES in northern Uganda (Doctoral dissertation).

Patel, F. (2015) Effects of Accounting Information System on Organizational Profitability. *International Journal of Research and Analytical Reviews,* 2,168-174.

Pike, R. H. (1986). The design of capital budgeting processes and the corporate context. *Managerial and Decision Economics, 7*(3), 187-195.

Pitt, Leyland; Watson, R. & Kavan, C. (1995). "Service Quality: A Measure of Information Systems Effectiveness," *MIS Quarterly*, (19: 2)

Pramod, D., & Raman, R. (2014). A study on the user perception and awareness of smartphone security. *International Journal of Applied Engineering Research, 9*(23), 19133-19144.

Pretorius, B., & Van Niekerk, B. (2015). Cyber-security and governance for ICS/SCADA in South Africa. In J. Zaaiman, & L. Leenen (Eds.), *Proceedings of the 10th International Conference on Cyber Warfare and Security* (pp. 241-251). Reading, UK: ACP.

Radaideh, Murad, 2010, Impact of Mechanical Processing on Accounting Information Systems: Applied Study in the Jordanian Customs Department, unpublished Master thesis, Al Al-Bayt University, Mafraq, Jordan.

Rajan, M. (2010). *Internet phishing hook, line and hopefully not sunk.* (MBA thesis). University of KwaZulu-Natal, Durban.

Ramezan, M. (2009). Measuring the effectiveness of human resource information systems in national Iranian oil companies and empirical assessment. *Iranian Journal of Management Studies, 2*(2), 129-145.

Richardson, R., & Director, C. S. I. (2018). CSI computer crime and security survey. *Computer Security Institute,* 1, 1-30.

Richardson, V., Smith, R., & Watson, M. (2019). Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems 33*(3): 227–265. https://doi.org/10.2308/isys-52379

Rodriguez, C. S., & Spraakman, G. (2012). ERP systems and management accounting: A multiple case study. *Qualitative Research in Accounting & Management, 9*(4), 398-414. https://doi.org/10.1108/11766091211282689

Saeidi, H. (2014) The Impact of Accounting Information Systems on Financial Performance: A case Study of TCS India. *Indian Journal of Fundamental and Applied Life Science*, 4, 412-417.

Said F. & Noha H. (2019). *Cyber-security measuring and assessment method for modern enterprises. pp* 158.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods:Business students, (4th edition).* England:Pearson Education Limited.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law, 12*(2), 1558-7215.

Seddon, P. B., Graeser, V., & Willcocks, L. P. (2012). Measuring organizational IS effectiveness: An overview and update of senior management perspectives. *ACM SIGMIS Database, 33*(2), 11-28.

Spathis, C. (2006). Enterprise systems implementation and accounting benefits. *Journal of Enterprise Information Management, 19*(1), 67-82.

Tanaka, H., Matsuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of E-local government in Japan. *Journal of Accounting and Public Policy, 24*(1), 37-59.

U.S. Department of Homeland Security (DHS). (2020). *National Initiative for Cybersecurity Careers and Studies.*

Venkatesh, V., Morris, M. G., Davis, G. B., &Davis, F. D. (2013). User acceptance of information technology: toward a unified view. *MIS Q.* 27, 425–478

Von Bertalanffy, L. (1968). *General system theory: Foundations, development, applications*. New York: George Braziller.

Von Solms, R., & van Niekerk, J. (2013), "From information security to cyber security", *Computers and Security*, 38, 97-102.

Wang, Y., Kannan, K., & Ulmer, J. (2013). The association between the disclosure and the realization of information security risk factors", *Information Systems Research,* 24(2) 201-218.

Whitty, M., Doodson, J., Creese, S., Hodges, D. (2015). Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychol. Behav. Soc. Netw.1 8*(1), 3–7

Wong, K. K. (2013). Partial Least Squared Structural Equation Modelling (PLS-SEM) Techniques using SmartPLS. *Marketing Bulletin*, 24(1), 1-32.

Xu, H., S. Guo, J. Z. Haislip, & Pinsker, R. E. (2019). Earnings management in firms with data security breaches. *Journal of Information System 33*(3), 267-284.

Yaseen, S. G., & Saleh, G. A. (2014). Evaluation of Accounting Information Systems in Jordanian Islamic Banks, *Scientific Journal of Faculty of Commerce, Asyoot University, Egypt,* 27, 18, 34-64.

APPENDIX 1

QUESTIONNAIRE

UNIVERSITY OF EDUCATION, WINNEBA

SCHOOL OF BUSINESS

MASTER IN BUSINESS ADMINISTRATION

DEPARTMENT OF ACCOUNTING

Dear respondent, I am a student of the University of Education, Winneba Business School. This questionnaire is intended to solicit data for academic purposes in partial fulfillment for the award of master in Business Administration Degree (Accounting). Your identity/name will not be referred to anywhere in the report. The information you give will be used purely for academic purposes.

Please respond to the following questions

SECTION A – DEMOGRAPHIC DATA

1. **Sex** (Please tick appropriately) Male [ ] Female [ ]
2. **Age** (Please tick appropriately)

   Below 20 [ ] 21-30 [ ] 31-40 [ ]

   41-50 [ ] Above 50 [ ]

3. **Highest Level of Education**

   A. Diploma [ ] B. HND [ ] C. First Degree [ ] D. Masters [ ]

   Other (please specify)…….

4. **The number of years working in the banking sector?**

   A. 1-5 years [ ]

   B. 6-10 years [ ]

C. 11-15 year [ ]

D. Over 15 years [ ]

5. **How often do you use Accounting Information Software/System? (** Please tick appropriately)

A. Daily [ ] B. Week-days (working hours) [ ] C. Monthly [ ]

SECTION B – EFFECTIVENESS OF ACCOUNTING INFORMATION SYSTEM

Please evaluate the degree of your agreement with the following criteria for assessing the effectiveness of accounting information systems:

Key: 1=Strongly Disagree; 2=Disagree; 3=Neutral; 4=Agree; 5=Strongly Agree

STATEMENT	1	2	3	4	5
System Quality					
The system is reliable					
The system is easy to learn and understand its features					
The response time for the system is fast					
The system is flexible					
Information Quality					
Management reports are reliable					
System output is clear and understandable					
The information from AIS improves the quality of work					
Service quality					
IT team provide support for the system					

IT team has technical competence					
Information system department is responsive, timely and reliable					
System Use					
Staff utilize the capabilities of an information system					
Appropriate use of the system					
Extensive use of the system					
Staff understand every function of the AIS					
User Satisfaction					
Users are satisfied with system report					
Users are satisfied with the IT team support					
Users are satisfied with AIS interface.					

SECTION C – LEVEL OF SECURITY AWARENESS

Please evaluate the degree of your agreement with the following criteria for assessing the effectiveness of accounting information systems:

Key: 1=Strongly Disagree; 2=Disagree; 3=Neutral; 4=Agree; 5=Strongly Agree

STATEMENT	**1**	**2**	**3**	**4**	**5**
Able to dictate or know when a computer is hacked					
Knows what an email scam is and how to identify one?					
Ant-virus currently installed, updated and enabled on your computer					
Uses the same password for your work accounts as					

you do for your personal accounts at home, such as Facebook, Twitter or your personal email accounts?					
Knows who to contact in case your software is hacked or if your computer is infected?					
Knows what is a phishing attack					

SECTION D – CYBERSECURITY PERFORMANCE

Please evaluate the degree of your agreement with the following criteria for assessing cybersecurity performance:

Key: 1=Strongly Disagree; 2=Disagree; 3=Neutral; 4=Agree; 5=Strongly Agree

STATEMENT	**1**	**2**	**3**	**4**	**5**
Analyze					
Accounting Information System easily identifies the type of cybercrime or cyber threat.					
AIS determines the nature of cybercrime or cyber risk.					
AIS provides details on all possible unauthorized system login					
Defend					
Accounting Information System is automated to avoid system hacking					
Accounting Information System serves as a security firewall to prevent cybercrime					
Accounting information System defends sensitive information from unauthorized use.					
Accounting Information System is programmed to avoid					

financial data loss.					
Detect					
Accounting Information System has the capability to signal staff of possible system hacking threats.					
Accounting Information System sends a notification message to IT security team of possible cybercrime threats.					
AIS easily identifies data or information that has been hacked.					
AIS detects an unauthorized system user login.					
Revival					
AIS is able to backup all hacked system data and information					
AIS is automated to restore software/system when hacked					
All document files are easily retrieved whenever Accounting Information System is hacked.					

THANK YOU FOR YOUR COOPERATION