UNIVERSITY OF EDUCATION, WINNEBA

ASSESSMENT OF INFORMATION TECHNOLOGY SECURITY MANAGEMENT SYSTEM: A CASE OF COLLEGES OF EDUCATION IN THE BONO REGION OF GHANA.

RUFIA ADAMS

MASTER OF SCIENCE DISSERTATION

2021

UNIVERSITY OF EDUCATION, WINNEBA

ASSESSMENT OF INFORMATION TECHNOLOGY SECURITY MANAGEMENT SYSTEM: A CASE OF COLLEGES OF EDUCATION IN THE BONO REGION OF GHANA.

RUFIA ADAMS

A dissertation in the Department of Information Technology Education, Faculty of Applied Sciences and Mathematics Education, submitted to the School of Graduate Studies in partial fulfilment of the requirements for the award of the degree of Master of Science (Information Technology Education) in the University of Education, Winneba

MAY, 2021

DECLARATION

STUDENT'S DECLARATION

I, **Rufia Adams**, declare that this dissertation except for quotations and references contained in published works which have all been identified and duly acknowledged, is entirely my original work, and it has not been submitted, either in part or whole, for another degree elsewhere.

SIGNATURE……

DATE……

SUPERVISOR'S DECLARATION

I hereby declare that the preparation and presentation of this work was supervised in accordance with the guidelines for supervision of dissertation as laid down by the University of Education, Winneba.

DR. KWAME ANSONG GYIMAH

SIGNATURE……

DATE……

DEDICATION

I dedicate my dissertation work to my family and many friends. A special feeling of gratitude to my loving parents, Mr. and Mrs. Adams, and husband, Nasirdeen whose words of encouragement and push for tenacity ring in my ears. My sisters Hiba and Najiba and brother Ahmed Salim have never left my side and are very special.

ACKNOWLEDGEMENT

I am thankful to Almighty Allah for his blessings for the successful completion of my dissertation. My heartiest gratitude, profound indebtedness, and deep respect go to my supervisor Dr. Kwame Ansong Gyimah, head of the department, Department of Information Technology Education, University of Education, Winneba (Kumasi Campus) for his constant supervision, affectionate guidance, and great encouragement and motivation. His keen interest in the topic and valuable advice throughout the study were of great help in completing this dissertation.

I convey my special thanks to the reviewers for their constructive review and guidelines.

Finally, I would like to thank my workplace colleagues especially the administrative staff of Al-Faruq College of Education, and my course mates for their appreciable assistance, patience, and suggestions during my dissertation.

TABLE OF CONTENTS

LIST OF TABLES

TABLE **PAGE**

ABBREVIATIONS

AFCOE	Al-Faruq College of Education
BECOLED	Berekum College of Education
COE	College of Education
I S	Information Security
I T	Information Technology
ISMS	Information Security Management System
SP	Server Provider
URL	Uniform Resource Locator
VPN	Vitual Private Network

ABSTRACT

Higher Educational institutions benefit greatly from information systems. Information security (IS) is an intense issue of the modern-day, it discusses the techniques and methodologies used to secure confidential, private, and sensitive information or data in print, electronic, or any other form against unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. As a result, to maintain a high level of performance and remain competitive, higher education institutions invest a significant amount of money and effort in obtaining and managing information. The purpose of this study is to give us a better understanding of Information Technology security, strategies and practices in Colleges of Education in the Bono Region of Ghana. This research was a case study of two Colleges of Education in the Bono Region. A total of 62 respondents were purposively sampled for the study. Online Questionnaires was used to achieve the study's objectives with the target population comprising Administrators, Tutors, and IT personnel of the selected colleges of education. The findings revealed that the information security programs had inadequate senior management support and oversight. With no education or training programs accessible to tutors in the Colleges of Education, there is poor knowledge of information security. The study concludes among others that, the majority of the groups at the examined Colleges of Education lacked adequate knowledge and security implementation, indicating the need to activate the administrators' duties to deploy a well-designed information security system. The study, therefore, concluded that, the colleges should organize training on information security for all staff to equip them with the required knowledge to manage information in the colleges.

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

In recent years, information technology (IT) security has become a growing field of study for most research works. As a result of the increasing number of security breaches, business and educational environments are becoming increasingly concerned. Several security approaches have been identified, and numerous approaches have been developed to address the major security issues about data and information protection. However, none of them were able to address all of the issues (Snyman & Kruger, 2021). IT security breaches are almost becoming ubiquitous with IT resources. IT security breaches have an internal and external effect on the operations and wellbeing of an organization. Internally, IT security breaches lead to the disruption of business and organizational operations. Unauthorized disclosure of information to persons who are not allowed to access such data remains the most common type of information security incident that colleges and universities face (Schatz & Bashroush, 2016; Yayla & Hu, 2011).

Computer systems have through the ages, become a need for most institutions where several institutions including schools and companies rely on for their daily routine activities. Higher educational institutions and other organizations, strongly rely on information systems for their daily operations including teaching and learning, running of their daily activities and, sharing information. These systems may hasten daily activities and bring about higher work output. Higher Educational administrators often work within the central administrative department and also in individual faculties, departments, and sections of universities and colleges of higher education (Eyadat, 2015).

As computer systems are being heavily utilized in universities and colleges to increase work output, so has information security become a basic requirement because distributed computing is inherently insecure due to the connection of these private networks to the internet (Adu, 2016). In an institution, one of the roles played by the administrators is to provide and put in place measures to ensure security in all aspects of the organization including computing infrastructure. However, the increase in the use of computer systems by institutions can influx new vulnerabilities and exploits which could render a fully patched system insecure and plagued with flaws.

The users are the weakest link, hackers use to break into an organization (Katz, 2005). Unintentional errors caused by users such as downloading from unknown sources can be considered high threats to information security in an organization (Whiteman & Mattord, 2012). Information security education, seminars, training, and awareness programs that continuously educate professionals and users on how to utilize the new and advanced security technology are needed.

Rezgui (2009) and Kandus (2011) have indicated, although there is the availability of information security technology and official organization standards, a massive percentage of higher educational institutions offer no information security programs to their staff. The process of protecting the higher education management system without compromising data privacy, accessibility, academic and intellectual freedom, which is at the heart of the higher education management system, is known as the information technology (IT) security system in higher education (de Bruijn& Janssen, 2017). It is all about maintaining data confidentiality, ensuring data integrity, and making data available to approved users on a timely basis. Despite the numerous security functions,

IT security in higher education continues to be an area of ongoing investment. Because of the diversity of stakeholders' interests, applications, technical advancements, and intrusions, it is impossible to say definitively that the educational sector is highly safe. According to the most recent pattern, higher educational institutions have the highest number among reported breaches of all sectors, implying increased possible attacks in the coming days (Africa Cyber Report. 2016). Assessing a higher education institute's IT security management system (for example, Colleges of Education in Ghana's Bono Region) will assist the institution in defining its current IT security management system, resulting in an improved IT Security management and execution process for the institution.

1.2 Statement of the Problem

Educational institutions store large amounts of sensitive data ranging from contact information (Registered Telephone Numbers), academic records, financial information, health records, and national identity records of both staff and students, making them vulnerable to targeted unauthorized interference and compromise (Troia, 2018). Higher Educational institutions often run systems with vulnerabilities and with little monitoring or management. The typical College research or teaching lab is managed by a faculty member who has many other responsibilities or by a student manager who may have had little training. According to Popa et al. (2011), Colleges of Education, as institutions that train qualified and professional teachers for the nation, have made numerous promises regarding the potential growth of education and research. However, they often face the challenge of what to do about IT security and where they should have put more emphasis. When most educational institutions carry out research;

confidentiality and ensuring secure distribution and integrity of their data is an utmost need in todays' excelling technological management system.

In today's life, there are continuous attacks on a big organization that allow access to the internal network, therefore resulting in the economic meltdown which causes loss of reputation and prestige (McCrohan, Engel & Harvey, 2010). Many higher institutions are among the most vulnerable to attacks and these attacks may include the theft of both students and staff information. This shows that cyber security and training must be included in any organization's security management plan. With proper awareness programs, training, educations, and policies, the higher institutions must also have measures in security, privacy, trust, audit, and legal requirement (Pastor, Díaz, & Castro, 2010). Berekum and Al-Faruq Colleges of Education store sensitive information and data on the colleges' computers but very little is known about the state of information security of these Colleges of Education in the Bono Region of Ghana. As a result, this study attempts to assess the information security management system in the Berekum and Al-Faruq Colleges of Education.

1.3 Research Objectives

The general objective of this study was to assess the information technology security management system in Colleges of Education in the Bono Region of Ghana. Specifically, the study ought to:

1. identify the Information Security Practices and Technologies in Colleges of Education in the Bono Region of Ghana.

2. evaluate the Information Technology Security Awareness Pattern in Colleges of Education in the Bono Region.
3. evaluate the present information security management system in Colleges of Education in the Bono Region.

1. 4 Research Questions

This research sought to find answers to the following questions:

1. What are the Information Security Practice and Technologies of Colleges of Education in the Bono Region of Ghana?
2. What is the Information Technology Security Awareness Pattern in Colleges of Education in the Bono Region?
3. What is the present information security management system in Colleges of Education in the Bono Region?

1.5 Limitations and Delimitations

It is important to note a couple of potential limitations and delimitations in this research. The study solely focused on the IT security policies, practices, and strategies being adopted in Colleges of Education in the Bono Region to secure their information assets and to create awareness in their users of security vulnerabilities.

This study was mainly focused on administrators of higher education settings in the Bono Region of Ghana. (i.e Colleges of Education) which are Al-Faruq College of Education, Wenchi, and Berekum College of Education which may limit its generalization due to financial and budgetary constraints since all the forty-six colleges of education were not included in the research. In addition, the ultimate findings will be delimited by geographic location. (i.e the sample will comprise of some selected

administrators who currently works in the Colleges of Education in the Bono Region of Ghana) since the researcher chose only colleges of education in the Bono region because of proximity and easy access to those institutions.

1.6 Organization of the Study

This research is presented in chapters with each chapter carrying a detailed description of activities. Chapter one includes the background to the study, the problem statement, the justification of the study, the study objectives, the research questions, and limitations and delimitations of the study. Chapter two consists of a review of related literature on the topic of study. The literature includes background information on information technology security and higher educational institutions.

Chapter three presents the methodology of the study. This includes the design, population, sampling techniques, and method of data collection. Chapter four outlines the findings from the research data gathered and analyzed. The presentation is in the form of frequency tables, and cross-tabulation where applicable. Chapter five which is also the last chapter contains the conclusions and recommendations made from the study.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The systematic description of information that is accessible can be described as a literature review. On the topic at hand, it aids in the gathering of information and insight into the chosen subject, as well as one's point of view, motive, or personal interest are not affected. This chapter is critical to ensuring that the literature review is comprehensive and does not take sides. Moreover, this chapter sheds light on the different methods and dynamics used in research on topics of a similar nature.

Within the boundaries of IT security strategy, policy, and practice, this chapter focused on reasons for users (administrators of higher education) to use the information security facility within the two Colleges of Education in the Bono region. Their IT security knowledge and actions were evaluated. In Ghana, users prefer all types of free internet services, especially those in academia, making them particularly vulnerable to information and data theft, such as mail id or social media account hacking, theft of personal and commercial data, images, and so on. In Ghana, as the number of internet users grows, so do the number of cases of data security breaches especially in the field of academia.

2.2 Background of Information Security

In 2016, nearly one percent of all emails sent were essentially malicious attacks, the highest rate in recent years (Global Cyber-security Index, 2017). Information security incidents are burgeoning due to a combination of technological, socio-economic, cultural, political, and legal forces. The safety buffer between systems, especially those

related to national security and critical infrastructure, was reduced significantly in an increasingly connected and complex global computing environment. Illicit internet activity has evolved into a strong black market for individual actors, criminal networks, and terrorists from a game for "internet trolls".

IT security breaches are almost becoming ubiquitous with IT resources. For many firms, it is not if but when - their IT resources will be breached. For example, a 2015 report by the US Government, accountability Office (GAO) indicated that the number of cyber security incidents reported by federal agencies to the US Computer Emergency Readiness Team (US-CERT) rose from 5,503 in 2006 to 67,168 in 2014, an overwhelming 1,121 percent increase (GAO, 2015).

Information Security can be the term in the broader aspect as the preservation of Confidentiality or protection from unauthorized use or disclosure of information. Also, Integrity that is ensuring data accuracy and completeness through protection from unauthorized, unanticipated, or unintentional modification, and including authenticity. Again, Availability is making data available to the authorized users on a timely basis and when needed. Preservation of confidentiality, integrity, and availability of information (Dodge, 2009: Ward & Hawkins, 2003). Also, other properties, such as authenticity, accountability, non-repudiation, and reliability can be involved (Fal, 2010). The currently relevant set of security goals may include confidentiality, integrity, availability, privacy, authenticity & trustworthiness, on-repudiation, accountability, and audibility (Cherdantseva & Hilton, 2013).

IT security breaches have an internal and external effect on the operations and wellbeing of an organization. Internally, IT security breaches lead to the disruption of business operations, negative stock market reactions (Schatz & B shroush, 2016; Yayla & Hu, 2011), lawsuits, a decline in sales due to reduced store and online customer patronage leading to deflated profits (Chai, Kim & Rao, 2011; Glazier, 2014) and hence fewer staff compensations' (stocks and monetary incentives) and eventually lower shareholders' payoffs.

Private information on administrators, staff, students, alumni, and research works (e.g., social security number, date of birth, driver's license number, financial and medical information, grades) is held in academic institutions. Also, academic institutions have always been at the forefront of research and development efforts for all technological innovations in the country. In certain cases, such private data and intellectual property are tightly regulated by security policies; however, there are huge loopholes. Information security vulnerabilities that can occur from the within (e.g. students, employees, faculty) or the outside (e.g. hackers, attackers, organized criminals) have generated significant problems about the networks of academia.

The vulnerability of the country to cyber-based incidents due to the increasing prevalence of broadband connectivity has resulted in data loss (Adu, 2016) and security awareness challenges. With little chance of detection, anyone with malicious intent will exploit the vulnerabilities of academic institutions. As targets in the private sector and government are better covered, offenders are turning to harder targets such as academia, home consumers, and mobile staff. Academic institutions are extremely attractive targets due to their distinctive characteristics (e.g., open culture, sensitive material, diverse users and access methods, and high-risk activities), as outlined.

Strictly based on technological developments may obscure other environmental variables that are drivers for Higher Education Innovation. The current Knowledge Management framework for Higher Education, which generates areas of opportunity drastic improvements, and commitment to protection are also pursued by (Yeo, Rahim & Miri, 2007). It has been more complex bringing everybody under the security protocol/policies because of more rapidity and dynamism in Technologies that are integrating nearly everyone (student and teachers) every day.

2.3 Information Security

Information security is about how to prevent attacks or failing that, to detect attacks on information-based systems. Security Attacks are broadly categorized into two types: Passive Attacks and Active Attacks. The passive attack is an attempt to learn or make use of information from the system but does not affect system resources, passive attacks are difficult to detect because they do not involve any alteration of the data while the active attack is mainly an attempt to alter system resources or affect their operation. The active attacks are subdivided into four categories namely: Masquerade: one entity pretends to be a different entity to affect operations. Replay: Capture of the data unit and its subsequent retransmission to produce an unauthorized effect. Modification of messages: Some portion of the legitimate message is altered to produce undesired results. Denial of service: Prevents normal use or management of communications facilities. The developed nature of Ghana's IT infrastructure and the pervasive use of digital technologies requires the development of policies for cyber security to prevent data losses and protect the national infrastructure from threats (Adu & Adjei, 2018). Threats to information and information systems may be categorized and a corresponding security goal may be defined for each category of threats. A set of

security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving management system. The currently relevant set of security goals may include confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability, and audibility (Cherdantseva & Hilton, 2013).

2.4 Higher Education Information Security System in Ghana

Higher education or Advanced level Education, post-secondary education, tertiary education, or education at the third level are the optional final period of formal learning after secondary education takes place. It is important to have an education at the undergraduate and postgraduate levels. Also delivered at academies, colleges, Higher education is also accessible through universities, conferences, and technology institutions. Some college-level institutions, including technical schools, business schools, and other professions, Colleges that grant technical qualifications or academic degrees. Technological development has brought about a rise in data volumes and has heightened the risk of sensitive data. These advances in information technology have rather rendered the data of higher institutions vulnerable and raised concerns over information security. Ransomware, phishing, malware, pharming, spyware, etc. have become a cliché in the IT fraternity presumably because of the devastating effect it has caused to organizations and some higher institutions (Adu, et al, 2018).

The Higher Education School Information Security management system mainly means knowledge management system: institutional incorporation into the social system to promote joint activities, technical and physical structures. Building knowledge, decision making, inference, or exploration. Social services can also be included. System of management: the community in which a person lives, and the people and institutions

with which they are interacting fundamentally, it is possible to summarize the management structure to be centered as a system of technical management and a non-technical system of management for the higher education field of today. It protects the internal and external customers, the device, and all the related stakeholders.

2.5 Risk Management of Data

For the security of data, they should be live on secure servers, be secured, for the safety of records. At rest and in transit, and available only via secure or HTTPS apps to administer. Though information security is one of the most serious threats to corporate data, administrators of higher educational institutions' carelessness concerning the management of data on USB drives may be concerning.

The common attacks and threats most institutions and their employees face are operating systems vulnerabilities, malware, phishing, identity theft, and privacy violation (Rao & Pati, 2012). Nthala et al. (2018) state that all these threats are usually mitigated well in large organizations because they have security policies, segmented network architectures, firewall, antivirus, intrusion detection systems, intrusion prevention systems, patching management, backup solutions, and IT support team.

To be an involved stakeholder in enterprise-level processes, programs, and services, access is essential Data. Role-based access and multifaceted administrative monitoring that enables workers to access Safe access to knowledge and mission-critical infrastructure should be established, understood, and sought. To protect systems and networks, local data centers should first be secured through Key/keycard, role-based access, and data center protection are formally tracked. Secondly, regular periodic,

systemic, and thorough security audits should be carried out. To identify management effort, Institutional identity management requirements goals should be coordinated to remain in line with the opportunity to handle personalities efficiently. A successful organizational information security policy should incorporate clear definitions of user responsibilities for information security (Gaunt, 2000; Whitman & Mattord, 2014).

The diverse roles of senior administrators in higher educational institutions provide unique insights into the production and integration of information security awareness perspectives at the departmental and faculty level, especially how information conversations across teams and workplace colleagues develop, how risk is assessed, how defenses are improved, and how overall decision-making to enhance how information security is made.

In today's evolving security threat environment, higher education institutions should consider creating a defensive shield to defend against internal information security risks initiated by employees' conduct, as well as external information security threats that can take advantage of employees' careless behaviour.

2.6 User Awareness/Education for Information Security

Information security has become one of the basic operational requirements of any type of organization, especially government organizations, and it entails safeguarding key information assets from security threats (e.g. unauthorized access, use, dissemination, corruption, or destruction) that could endanger its availability, integrity, and confidentiality (Gulappagol & ShivaKumar, 2017; Moon et al., 2018).

To raise awareness among users, one should be an advocate of self-education about data security and effective fortification. Regarding security issues for users (students and teachers) administrators for the higher educational institution can then inspire the adoption of intelligent Practices in security by discussing personal security issues at the same time as internal security Issues with protection. User education is done by engaging them in activities that raise awareness among users. The Institute should have well-written, easy to read and generally understood notices for the user awareness of security practices regarding data.

In the case of Ghana, the government in 2008 and 2012 passed the Data Protection Act, 2012 (Act 843) and the Electronic Transaction Act, 2008, Act 772 respectively, to ensure the security and management of data in the country. The Data Protection Act of 2012 (Act 843) is based on the basic rule that anyone processing personal data must consider the individual's right to privacy in his or her communications. The Act poses important data protection concerns and requires data controllers to take the required precautions to protect the privacy of personal data under their control. Determine the internal and external threats to personal information in that person's possession. Put in place and maintain adequate protections against the threats that have been found.

Accessed security policies for administrators of higher educational institutions, however, good policies can not necessarily turn into good practices. Confidentiality, Compliance enforcement can be tracked, and rules enforceable. Whether Strategy Compliance can neither be tracked nor enforced and the policy data can then be repackaged prudentially. Formally monitored may be as guidelines or suggested use/behavior. Information security policy is needed to inform individuals who operate

within an organization to conduct themselves properly concerning information security issues (Julisch, 2016).

Secondly, there should be routine periodic, systematic, and thorough security audits. To identify management effort, Operational goals for requirements for management should be set to be in tune with the ability to be effective Current Scale, Scope and Diversity of Information Security System in Higher Educational Information security fortification System of Colleges of Education in the Bono region of Ghana.

Recently, the culture of antivirus non-installation and Internet encryption or improper use of USB flash drives has resulted in most colleges facing hazardous IT security hazards. When the IT management system officials are faced with novice and rudimentary IT culture, a proven or unknown effort to hack the results, ratings, question papers intended for continuous assessments, secure data is not impossible. The cases referred to above have shown the significance of a robust IT protection strategy, policy, and climate in the context of higher education institutions, especially in the Bono region of Ghana and particularly, in the Colleges of Education. The need for information security awareness is increasingly important due to the limited knowledge in information security issues (de Bruijn & Janssen, 2017) and the overarching dependence on Information and Communication Technology (ICT) across organizations (Zhao, 2016).

From the point of view of developing countries such as Ghana, which is emerging in the IT sector in securing its essential data, due importance must be paid exponentially. Colleges of Education and Higher Educational Institutions are most vulnerable to distributing large research-related data or a large number of questions each year,

confidential data related to question papers and answers for competitive exams, seminars, symposium papers, related study materials, and any worthy writings, etc. For the reasons discussed above, this study was undertaken to assess the IT security environment of some selected Colleges of Education in the Bono Region which are Al-Faruq College of Education and Berekum College of Education.

2.7 Recent Development of Information Security System Affecting Higher Educational Information Security Fortification System

Given the complex nature of individual behaviour and the various dimensions of a security vulnerability in organizational settings (Sebescen & Vitak, 2017), relying completely on security-related technologies is insufficient to reduce all types of security risks and elevate the information security level of organizations in general. The insufficiencies of technical controls in a context where human intervention and insider threats (Ho et al., 2018) are so critical is well summarized by (Schneier, 2011) in the assertion that "if you think technology can solve your security problems, then you do not understand the problems and you don't understand the technology". In this sense, the effective role of non-technical information security interventions, namely, information security awareness, is emphasized by a variety of studies in the field (Bulgurcu et al., 2010; Haeussinger & Kranz, 2013; Siponen, 2000) as a form of deterrent information security measure (Tipton & Krause, 2007).

Kim, Mims, and Holmes (2006) indicated that college of education students possess basic knowledge of most information security issues. In the same report, they recommended that institutions should provide easily accessible security training programs for their students to have effective Information Security program. Another recent case study conducted by (Bere, 2013) examined E-learning (Electronic learning)

by exploring the pedagogical application of WhatsApp mobile software. Bere (2013) suggested that mobile security threats negatively affected the usage of the WhatsApp application for learning. The suggestion was based on several factors. The concern of security was one of the most challenging factors. Fatani, Zamzami, Aydin, and Aliyu, (2013) approved that security issues affected the privacy of students' data. They also indicated that students' awareness level was low. Moreover, Androulidakis and Kandus (2011) and Eyadat and Al Sharyoufi (2014) revealed in their studies that users were unaware of the necessary measures to avoid possible unauthorized access and/or sensitive data retrieval from their devices, which indicated the lack of knowledge in securing the protection of their data and information. According to Kim, Mims, and Holmes (2006), deploying the emerging technologies successfully required the awareness of the security issues that might encounter while using these technologies. Therefore, proper Information Security program awareness should be available for institutes' on-campus and off-campus users of technological devices. The notion that a successful information security awareness program must be based on improving employees' cognitive frames of reference is well established especially when training is problem-centered (Pawlowski & Jung, 2019), and designed with an emphasis on appropriate security practices that improve online behavior (McChrohan et al., 2016), therefore aiming at reducing organizational insiders' cyber-risk behavior.

Normal trends suggest that Higher Education sectors appoint their Chief IT officer(s) who ensures that the hard securities are completed as they are easy to install and visualize. Though some of the cases the organization might not agree to expense some extra money on the not so imminent threat of IT security breach and compromise security (Arafat & Daiyan, 2012). Soft intervention on the other hand is not so easy to implement, while the development in the IT sector is still in a growing stage. Most of

the budget are not been allocated for strategy devices, decision-making. Policymaking, standard operating policy generation, risk assessment, awareness program, and management aspect. Normally everyone forgets that humans are the weakest link in the IT security chain and gives the least priority to human aspects of security planning. Therefore, considering the above scenario this research suggests an assessment of the IT security fortification management system of Colleges of Education in the Bono Region of Ghana.

2.8 Major Focus of I T Security Fortification System

Information security is a critical issue in all organizations. The success of information security in institutions depends, to a large extent, on the effective behavior of administrators, librarians, users, and all human staff (Amini, & Saberi. 2021).

In terms of information security knowledge, reducing exposure to information security hazards is not solely the responsibility of the information security professional. It is not the responsibility of the information technology (IT) department, rather, it is the responsibility of all departments.

In higher education, where a great deal of information is required for teaching and research, honesty and availability level, but low confidentiality level. Various studies National and international project work, paper, journal, thesis work, criteria for research, paper, journal, all of which are of tremendous significance and must not be breached, leading to any protection Incidents with breeches. Consequently, soft interventions covering strategy, policy, and experience are the major issues at the Institute of Higher Education concerning ensuring IT data security safety. Mostly the emphasis appears to deviate from the above-mentioned security approach of the

moment and thus causing an unhealthy structure of IT management. Experts have often stressed the focus on Continuous monitoring of the control system that is vulnerable and risk assessment from the community of IT consumers, in many instances. The tendency in the case of an educational institute the non-permanent existence of students and faculty members is more than just because of it.

2.9 Economic Crises that Higher Education Sector Faces in their Quest for a Robust Information Security Fortification System

Despite an increase in the use of information technologies across organizations, alongside the persistence of human behaviour-related threats such as social engineering (Hanus et al., 2018), limited action is taken to increase end users' information security awareness (Aloul, 2012).

Various higher education approaches to IT security are causing an unclear IT security fortification management system. The experts have always placed the focus on constant monitoring and risk assessment of the re-established management framework. Information Technology Security Administrators should plan to devote approximately One-third of their time to deal with technological considerations. The two-thirds left should be spent on developing policies and procedures, conducting security evaluations, and evaluating Risk, response to contingency planning, and security awareness promotion. Information security awareness is considered as a protection factor against employees' potential lack of knowledge about security threats they might fall victim to, without proper identification or detection in advance (Raneem & Jorge, 2020).

With the rapid development of information technology (IT) including smartphones, computers, tablets, smart watches, and the Internet of Things (IoT), providing security for home digital devices and services has become more essential and more challenging as many home users face online threats and attacks (Nthala et al., 2018). Experts have often stressed the focus on continuous management system monitoring and risk assessment that respond to meet the expectations of students and faculty members of contemporary consumer technologies and Communications: Students and faculty not only expect this to happen but there should be capable of using their academic smartphones, laptops, and consumer-based applications live, but still expect the programs of their institutions to work as elegantly and efficiently as desired. Three factors depend on the degree of security: the risk you are willing to take, the System functionality, and the expenses that you are prepared to pay.

2.10 Research Paradigms

The research paradigm can be called the way of thinking where a decision of this worldview generally relies upon analysts' reasoning and accepts to pick what direction to go and how to lead the planned examination where each worldview is valid on the ground of the expected task. According to Taylor, Kermode, and Roberts (2006), a paradigm is a broad view or perspective of something. Thomas Kuhn who is known for the term paradigm portrays a paradigm as an incorporated bunch of meaningful ideas, factors, and issues appended with comparing methodological methodologies and devices. It is important for the analyst to comprehend the philosophical situation of examination issues and to comprehend the diverse mix of exploration strategies. There are mainly three types of paradigms to understand reality. Positivism: The positivist paradigm of exploring social reality is based on the philosophical ideas of Aristotle,

Emmanuel Kant, and August Comte (Mertens, 2007). It is also known as scientific research or scientific method. This approach emphasizes observation and reason as means of understanding human behaviour. According to this paradigm, researchers are interested to collect general information and data from a large social sample instead of focusing on details of the research. Researchers' convictions have no incentive to impact the exploration study. The information depends on the experience of detects and can be acquired by perception and trial. Positivistic masterminds received his logical strategy as a method for the information age. With the suspicions and gained information, a definitive objective is to incorporate and orderly discoveries into an important example or hypothesis which is viewed as provisional and not a definitive truth. The positivistic paradigm has influenced educational research in the last half of the twentieth century. It regards human behavior as controlled and determined by an external management system. Hence human beings are driven without their intention, individualism, and freedom taken into account in viewing and interpreting social reality.

Interpretivism: It can be referred to as Social Constructionism in the field of management research. With the help of this philosophy, researchers focus to highlight the real facts and figures according to the research problem. This kind of philosophical approach understands specific business situations. In this approach, researchers use small samples and evaluate them in detail (Singh & Kasi, 2009). Realism: This research philosophy mainly concentrates on the reality and beliefs that are already existing in the management system. Direct reality means, what an individual feels, sees, hears, etc. On the other hand, in critical realism, individuals argue about their experiences for a particular situation (Sekaran & Bougie, 2010). This is associated with the situation of

social constructivism because individual tries to prove his beliefs and values. In this research both the positivism and realism approach has been used. These approaches are very popular for researching this one. Though there are many more modern approaches available nowadays the progressive research specialists still have their faith glued to them. Because these approaches are very convenient for any kind of environment and have the ultimate ability to suit any major field of technology and social sciences. Also, they are very cost-effective which gives the researchers a positive edge. This research had not enough time constraints or budget to gather the views or opinions of all the concerned users, which is all the forty-six public colleges of education in the country for her research. The researcher had to interview with a group of concerned people which were administrators and I T heads in the two colleges of education to get their opinion on his/her research. That is the process that enabled the researcher to collect data and information from a convenient social arena. Thus this approach leads the researcher to a positivism research approach.

2.11 Identified Knowledge Gaps

Information security education areas are designed at the national and institutional levels, including innovative approaches to teaching information security, evaluations of existing approaches, emerging needs for information security curricula, innovative approaches to faculty development and capacity building, and other topics relevant to information security education (Bae, 2018).

This study found that human beings are the weakest link in IT security measures taken in this way. All previous research revealed that firewalls and policies were in vogue and research on. The conventional approach to information security education focuses on information security training and testing of information security awareness. While

the failure rate remained alarming, they provided mixed feedback. A mixed but balanced approach tends to lead to all possible dynamics and dynamism. A changed system of management. However, no concrete decision on any solution could be made. We tend to increase our interest in an integrated approach to the IT security management system, where the knowledge of management was blended into the IT management system. Also, higher levels of Educational Institutes, which have been largely exposed to the recent security breach incident, as they have a larger IT/user network, need additional attention. Inculcating the two features, one gave us the scope to evaluate such an institution's IT security management system that has IT-based learning and growth for its user rapidly.

2.12 Summary

The simplest safety model was to define each aspect of the organization or institution by its respective security model. Management of the structures, higher educational institutions should appoint an individual responsibility for IT security and these key responsible personnel should report to them of any security in data related to the institution. Information security education not only relies on IT but also depends on users' behavioral perspectives regarding information security (Tang et al., 2016).

A certain level of security certification should be established by the respective senior management of institutions or organizations, even now, although certification is proof of knowledge, but shows that you have put your time and effort into it. Acquiring specialized skills and the salary trends of these IT security personnel were further investigated. It was very difficult to define the exact enterprise security processes or technical resources higher specifications are required to improve the IT security

infrastructure around the campus arena of an institution or organization. Another recent study conducted by (Nthala et al. 2018) revealed that there is a clear need to develop a usable convenient tool that can be used by non-experts to manage the security configurations for different devices and services at home which could motivate administrators for better security and simplify the task for them.

The level of information security knowledge referred to how well employees understand the significance and consequences of information security policies, laws, and guidelines, as well as how well they follow them. The higher educational institution had been largely exposed to the recent security breach incident, which needed extra attention because they have a larger IT/user network. Inculcation of the two aspects in one gave us the scope to evaluate IT security. Educational management system since tools are complex and rely on field and type of use or Violations. The IT security system around the higher-level educational arena needed to be improved. Educational Institutions, which had been largely exposed to the recent security breach incident, as they had a wider IT/user network, needed additional attention.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter discusses the method adopted by this research. The chapter again mentions every component in conducting this research from a population, population frame, and sampling techniques used for the research. Finally, this chapter provides a detailed explanation of the selected mode of analysis used and the data collection method.

3.2 Profile of the Study Area

Al-Faruq college of Education and Berekum College of Education which are both situated in the Bono Region of Ghana happen to be the only Colleges of Education in the Region that train qualified teachers for the Region and the entire nation. Berekum College of Education was established in February 1953 with the vision of being an icon of excellence in teacher education in Ghana. Al-Faruq College of Education is the first Islamic College of Education established in 2015 to run teacher education programs. The College became a public institution in 2016 and is affiliated with the University for Development Studies. Programs offered by the two colleges of Education are B.ed Early Grade Education, B.ed Primary Education and B.ed J H S Education with specialties in ICT, Mathematics, Science, Music & RME, Social Studies, Arabic and English which students are all trained basically to be placed in the basic school level. All the Colleges of Education have well established IT departments that serves both students and tutors. In Berekum College of Education, there are a total of 6 staff whilst Al-Faruq College of Education has 4 staff in the IT department who is in charge of maintaining the hardware and software of the entire college.

3.3 Research Design

The research design refers to the overall strategy utilized to carry out research that defines a succinct and logical plan to tackle established research question(s) through the collection, interpretation, analysis, and discussion of data (Claybaugh & Zach, 2018). A research design is a framework that has been created to find answers to research questions (Tobi et al., 2018). Burns and Grove (2001) stated that designing a study helps researchers to plan and implement the study in a way that could help them obtain the intended results, thus increasing the chances of obtaining information that could be associated with the real situation.

The research was mainly a quantitative approach; however, the qualitative approach was used in a few instances. The quantitative research process was used to collect the data and it focused more on counting and classifying features and constructing statistical models and figures to explain what was observed. It was used to quantify the problem by way of generating numerical data or data that could be transformed into usable statistics. It was used to quantify attitudes, opinions, behaviors, and other defined variables and generalized the results to the study population. Quantitative Research uses measurable data to formulate facts and uncover patterns in research. Quantitative data collection methods are much more structured than qualitative data collection methods (Bryman, 2012). With the quantitative data analysis method, an online questionnaire was issued to respondents, that is the administrators and other staff members of the two colleges of education in the Bono region to gather their views on how information security was fortified and ensured in their respective colleges of education. According to Almeida (2017), a qualitative approach intends to understand a complex reality and the meaning of actions in a given context. This qualitative technique for gathering data

is used when the interviewer wants specific information, but also wants to find out what others think and know, without imposing his or her worldview on the interviewee.

3.4 Study Population

Reid (2012) described the population in a study as all units possessing certain characteristics, which are of interest to the researchers' study. From the definition, a population can be explained as the targeted community or group of people who are involved or selected by the researcher for his/her study. A population is therefore the pool of individuals from which a statistical sample is drawn for a study. For this research, the population used was drawn from Al-Faruq and Berekum Colleges of Education staff members. The population from which data were collected consisted of administrators and other selected staff members of Al-Faruq college of Education, Wenchi, and Berekum College of Education both located in the Bono Region of Ghana where information security plays a major role in their job description. The study population was 90 staff of the College of Education.

3.5 Sample Size and Sampling Technique

Purposive sampling, which is a non-probability sampling method, was used to select the sample from the population. Purposive sampling was formed by the discretion of the researcher, it purely considered the purpose of the study, along with the understanding of the target audience for the research. It is a nonrandom technique that does not need underlying theories or a set number of informants. Unlike the probability sampling method, the non-probability sampling technique uses non-randomized methods to draw the sample. The non-probability sampling method mostly involves judgment. Instead of randomization, participants are selected because they are easy to

access (Andale, 2015). In purposive sampling, the researcher decides what needs to be known and sets out to find people who can and are willing to provide the information by knowledge or experience. Purposive sampling is especially exemplified through the key informant technique, wherein one or a few individuals are solicited to act as guides to a culture (Lewis & Sheppard, 2006).

According to Yamane (1973) in calculating the sample size from the entire population, assuming a 95% confidence level and P = 0.5. The margin of error (amount of error that can be tolerated) used is 5% which is the standard used for social scientists and some physical scientists. Thus the formula is given by

$n = N/1+N (e)^2$

Where n = sample size

N = population

e = margin of error

The two Colleges of Education had a total population of 90. Therefore, n = 90/ (1+90) $(0.5)^2$

= 73 sample size.

However, a total of 62 respondents answered the questionnaire for the study. According to Garcia (2006), a sample size of 50% of the study is representative enough to generalize study findings to the study population.

A very important part of this research was the opinion of the IT persons/personnel and administrative staff in charge of students' data and examination results of the colleges and those were greatly emphasized. All the other administrative staff from the different category that is non-teaching staff that was not in the I T department had a set of

questionnaires with a few similarities with that of the IT staff and which did not make a big difference in the final findings of the research.

The primary advantages of this sampling approach were that it enabled us to access the samples at a convenient time, and the focus groups allowed us to have in-depth discussions, which further assisted us in logistically analyzing the research variables and correlating them appropriately to draw a rich conclusion. The primary disadvantage was that, due to easy sampling, the responses do not accurately reflect the perceptions of the various user groups that could have been collected if stratified sampling had been used, creating a paradox in generalizing the actual study results. Furthermore, determining the truth from all of the samples took a significant time.

3.6 Research Instrument

For this study, online questionnaires were used as the research instrument. The questionnaire consisted of 4parts. The questionnaire consisted of closed and open-ended questions, check-list questions, and a four-point Likert scale and was divided into 4parts as follows:

PART 1: The first part of the questionnaire was the demographic information of the respondents and organizational information. Queries about the personal information of the respondents were gender, age, and educational background.

PART 2: The second part of the questionnaire posed questions on Information Security practices and Technologies adopted by the respective colleges of education. This part also used checklist questions.

PART 3: In the third part, the questionnaire was on questions of I T Security awareness Pattern. How informed were the staff and administrators on the awareness of information security system management in their respective colleges of education using a four-point Likert scale with the questionnaire? A Likert scale is a psychometric scale commonly involved in research that employs questionnaires. The Likert scale was named after an American social scientist Rensis Likert, who devised the approach in 1932 (Norman, 2010). It is the most widely used approach to scaling responses in survey research. It is a rating scale that lets respondents select answers ranging across a spectrum of choices to gain deeper insight into attitudes, beliefs, or opinions (Norman, 2010).

PART 4: This part consisted of the Evaluation of the present information security management system in the colleges and the comments and suggestions of the respondents to the questionnaire.

3.7 Pre-Testing

After designing the questionnaire, the researcher printed hard copies and tested them using ten (10) respondents from the St Joseph's College of education in Bechem in the Ahafo Region. The challenges that were associated with the understanding of respondents regarding the questions were revealed through the pre-testing revealed. It was also through the pre-testing that, corrections were made in the questionnaire and ensured that it still achieved the study objectives.

With the reliability, which is the consistency of the measure of the observation, which the general rule of thumb says that the Cronbach's alpha of 0.6-0.7 indicates an acceptable level of reliability, and 0.8 or above indicates very good reliability for an observation.

Table 1: Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.816	.796	20

The table above shows very good reliability which is 0.796 for the 20 variables in the questionnaire. It means that internal consistency is at a high level for all the variables.

3.8 Data Collection Technique

The researcher sent the link of the questionnaire to the respondents in the two colleges of education through a social media platform, specifically, WhatsApp. The respondents were given some period to complete the questionnaire at their convenience. The questionnaire consisted of both open-ended and close-ended questions. The open-ended questions gave respondents the choice to determine the level of detail and length of some accounts to enable the researcher to understand their point of view. The open-ended questions also permitted the respondents to give a more adequate presentation of their understanding or appreciation of the issue under study and convey flexibility in their choice in an unstructured way, hence providing a kind of qualitative data. Conversely, to limit other responses to specific choices while curtailing the risk of misinterpretation, close-ended questions were used.

3.9 Data Analysis

The data was first exported from Google form into Microsoft Excel version and was then edited and exported into the Statistical Package for Social Sciences (SPSS) for analysis. Internal consistency checks were ran to pick out errors that were not noticed or picked during data validation, this provided an inherent consistency in the output of

the variables. Descriptive frequency tables and cross-tabulations were used to present the results. Qualitative data was presented in themes using thematic analysis.

3.10 Ethical Consideration

Approval for the study was sought from the Management of the two Colleges of Education. Informed verbal consent was also sought from every participant before the questionnaire was given out to them. Participants were informed of their right to opt out anytime in the course of the interview. Confidentiality was maintained on any information obtained from the participants. Names were not included in the questionnaires and codes were used for identification purposes. The researcher also ensured that participation in this study was purely voluntary, without any element of coercion. To ensure privacy, questionnaires were issued to respondents to fill in their free time devoid of any third-party involvement. Data collected were treated as confidential and participants were informed that the filling of the questionnaires took only 10- 15 minutes of their time.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents an analysis and discussion of the data collected from the field for the study. The presentation includes the demographic characteristics of the respondents and the study objectives. Frequency distributions are used to present some of the data.

4.2 Results

4.2.1 Demographic Characteristics

Table 2: Gender

	Frequency	Percentage
Male	50	80.6
Female	12	19.4
Total	**62**	**100.0**

Source: Field survey, 2021

Of the 62 respondents, 80.6% was males and 19.4% was females

Table 3: Educational Background

	Frequency	Percentage
BSc/BA/B.Ed/BBA/BTEC	34	54.8
MA/Med/MSc/MTEC/Mphil	26	41.9
PhD	2	3.3
Total	**62**	**100.0**

Source: Field survey, 2021

Of the 62 respondents 54.8% had attained Bsc/BA/B.E.d/BBA/BTEC, 41.9% had attained MSc, Mtec, Mphil, while those with an educational background within or above Ph.D. was 3.3%.

Table 4: Staff Category

	Frequency	Percentage
Academic	41	66.1
Non-academic	21	33.9
Total	**62**	**100.0**

Source: Field survey, 2021

Of the 62 respondents, 66.1% were those from the academic department whilst 33.9%was from the non-academic department.

4.2.2 Information Security Practice and Technologies

Table 5: How often does the College update the Operating System (Windows) of administrators

	Frequency	Percentage
Set to update automatically	22	35.5
At least twice a week	3	4.8
At least once a month	24	38.7
Never	13	20.9
Total	**62**	**100.0**

Source: Field survey, 2021

Of the 62 respondents, 35.5% of them indicated that the operating system of administrators is set to update automatically, 4.8% of them said it is updated at least twice a week, 38.7% of them said it is updated at least once a month and 20.9% of them said it is never updated.

Table 6: Anti-virus software installed on the College's computers

	Frequency	Percentage
Yes	39	62.9
No	9	14.5
Don't know	14	22.6
Total	**62**	**100.0**

Source: Field survey, 2021

Of the 62 respondents, 62.9% of them said anti-virus software is installed on the colleges' computers, 14.5% of them said anti-virus software is not installed on the colleges' computers whilst 22.6% had no idea about it.

Table 7: Person responsible for installing and maintaining security software on the computers in the college

	Frequency	Percentage
Administrator	12	19.4
IT staff	44	71.0
other staff	6	9.7
Total	**62**	**100.0**

Source: Field survey, 2021

Of the persons responsible for installing and maintaining security software on the computers in the college, 19.4% of the respondents said the administrators are responsible, 71.0% of them said the IT staff are responsible whilst 9.7% of them said other staff is responsible.

Table 8: How secure the college network is

	Frequency	Percentage
Very secure	3	4.8
Secure	29	46.8
Not secure	12	19.4
Don't know	18	29.0
Total	**62**	**100.0**

Source: Field survey, 2021

Concerning the security of the college network, 4.8% of the respondents said it is very secure, 46.8% of them said it is secure, 19.4% of them said it is not secure and 29.0% of them said they do not know.

Table 9: Security measures that the college has implemented

	Frequency	Percentage
Intrusion Detection system	11	17.7
File encryption	12	19.4
Antivirus	23	37.1
Others	16	25.8
Total	**62**	**100.0**

Source: Field survey, 2021

Of the type of security measure that the colleges have implemented, 17.7% of the respondents indicated an Intrusion Detection system, 19.4% of them indicated file encryption, 37.1% of them indicated antivirus and 25.8% of them indicated other measures.

Table 10: Greatest information security risk in the college in which data/information is easily lost to

	Frequency	Percentage
Incorrect Configuration	10	16.1
Internet downloads	26	41.9
Email viruses	13	21.0
Other	13	21.0
Total	**62**	**100.0**

Source: Field survey, 2021

Of the greatest information security risk in the college in which data/information is easily lost, 16.1% of the respondents indicated incorrect configuration, 41.9% indicated internet downloads, 21.0% of them indicated email viruses and 21.0% of them indicated others.

4.2.3 IT Security Awareness Pattern

Descriptive statistics were used to analyze the IT awareness pattern of the respondents. Standard deviations and means were used to explain the outcomes of the variables in the descriptive statistics. The mean is the arithmetic average of the responses on a scale of 1 to 4. The standard deviation (Std.) indicates how the data is spread out from the mean (Ali & Bhaskar, 2016). For this study, a mean greater than 2 indicates strong disagreement, and a mean of 2 or less indicates an agreement.

Table 11: Descriptive Statistics

Statement	N	Mini	Max	Mean	Std. Deviation
Availability of I T security policies that are clear and easy to read	62	1.00	4.00	2.5000	.76287
Administrators in my college adhere to its I T process or security standards	61	1.00	4.00	2.3770	.71096
The college has the level of information security we need to inspire confidence in our staff members	62	1.00	4.00	2.4516	.71695
Higher administrators' computers in my college have been monitored through the IT UNIT	62	1.00	4.00	2.4839	.78389
College provides me with a confidential repository for our classified data/information	62	1.00	4.00	2.5323	.71787
College provides staff training to raise information security awareness	62	1.00	4.00	2.6129	.75433
College adhere to I T process or security frameworks and or standards	62	1.00	4.00	2.3548	.74870
Senior management/ Administrators are actively involved in our college's information security issues.	62	1.00	4.00	2.5161	.74089
Presentation &discussions have raised my awareness of information security attacks in my college.	62	1.00	4.00	2.3548	.77028
Valid N (listwise)	61				

Source: Field survey, 2021

Most of the respondents disagreed that there is the availability of I T security policies that are clear and easy to read (mean = 2.500, stddev = 0.76287). Also, most of the respondents disagreed that administrators in their college adhere to its I T process or

security standards (mean = 2.3770, stddev = 0.71096). Again, most of the respondents disagreed that the college has the level of information security they need to inspire confidence in their staff members (mean = 2.4516, stddev = 0.71695). Furthermore, most of the respondents disagreed that higher administrators' computers in the colleges been monitored through the IT UNIT (mean = 2.4839, stddev = 0.78389). Most of the respondents also agreed that the colleges provide them with a confidential repository for their classified data/information (mean = 2. 5323, stddev = 0.71787). Also, most of the respondents agreed that the colleges provide staff training to raise information security awareness (mean = 2.6129, stddev = 0.75433). It was also disagreed by most of the respondents that the colleges adhere to I T process or security frameworks and or standards (mean = 2.3548, stddev = 0.74878). Most of the respondents again disagreed that the senior management/Administrators are actively involved in the colleges' information security issues (mean = 2.5161, stddev = 0.74089). Lastly, most of the respondents disagreed that presentation and discussions have raised their awareness of information security attacks in their colleges (mean = 2.3548, stddev = 0.77028).

4.2.4 Evaluation of present information security management system

Table 12: Factors that have been put in place to ensure colleges' information security

	Frequency	Percentage
I T steering Committees	19	30.6
Better staff information security awareness	14	22.6
Advanced security technology	8	12.9
Advanced security technology, Better staff information security awareness, Advanced security technology	7	11.3
I T steering Committees, Better staff information security awareness	9	14.5
I T steering Committees, Advanced security technology	1	1.6
Better staff information security awareness, Advanced security technology	4	6.5
Total	**62**	**100.0**

Source: Field survey, 2021

Of the factors that have been put in place to ensure information security in the colleges, 30.6% of the respondents indicated the institution of I T steering Committees, 22.6% of them said better staff information security awareness, 12.9 of them said the use of advanced security technology, 11.3% of them said advanced security technology, better staff information security awareness and advanced security technology, 14.5% of them said the institution of I T steering Committees and better staff information security awareness, 1.6% of them said the institution of I T steering Committees and the use of advanced security technology, and 6.5% of them said Better staff information security awareness and advanced security technology.

Table 13: How difficult is it to convince management to invest in securing a strong fortified information security network

	Frequency	Percentage
Very easy	2	3.2
Easy	21	33.9
Very difficult	22	35.5
Difficult	17	27.4
Total	**62**	**100.0**

Source: Field survey, 2021

As to difficult is it to convince management to invest in securing a strong fortified information security network, 3.2% of the respondent said it is very easy, 33.9% of them said it is easy, 35.5% of them said it is very difficult and 27.4% of them said it is difficult.

The respondents were asked what they think will help improve the information security levels of the colleges. Most of the concerns were about awareness creation and infrastructural development. Below are some of their views:

"To establish an active department of the unit and the provision of IT Infrastructure."

"They should organize a workshop on that and also management should have the willingness to take experts advise."

"Creating proper awareness of the management on IT security and the need to invest in IT at the college"

The respondents had other concerns regarding information security in their College. The concerns were about means of strengthening the security information in the colleges. Some of these concerns are given below:

"More ICT equipment should be procured and qualified and competent persons should be employed"

"There should be antivirus software for all computers and it should be updating regularly"

"I suggest that to have a very strong information security at colleges, authorities should handle that task separately from administration work"

"Colleges should invest in Information Security Systems to secure their data/information"

"People have less information on information security and its high time awareness is created to let people be on the alert."

4.3 Discussion

4.3.1 Information Security Practice and Technologies

The majority (38.7%) of the respondents indicated that the operating system of administrators is updated at least once a month. The college regularly update their system administrators' machines at least monthly. This will prevent the vulnerability of the operating systems. This is in line with the assertion by Rao and Pati (2012) that the common attacks and threats most institutions and their employees face are operating systems vulnerabilities.

Also, the majority (62.9%) of the respondents indicated that anti-virus software is installed on the colleges' computers. The issue of antivirus non-installation has resulted in most colleges facing hazardous IT security hazards. This is in agreement with de Bruijn and Janssen (2017) that significance of a robust IT protection strategy, policy, and climate in the context of higher education institutions.

Again, the majority (71.0%) of the said the IT staff are responsible for installing and maintaining security software on the computers in the college. The two colleges of education have a well-organized IT department led by the IT manager and administrators, as well as an IT technician and IT staff assigned to particular responsibilities. This agrees with (Gaunt, 2000; Whitman and Mattord (2014) that a successful organizational information security policy should incorporate clear definitions of user responsibilities for information security.

Furthermore, the majority (46.8%) of the respondents said the college network is secure. Of the type of security measure that the colleges have implemented, most (37.1%) of the respondents indicated the antivirus. This security might be due to some security policies including the antiviruses that are installed on the computers. This agrees with the view of Nthala et al. (2018) who stated that threats are usually mitigated well in large organizations because they have security policies, segmented network architectures, firewall, antivirus, intrusion detection systems, intrusion prevention systems, patching management, backup solutions, and IT support team.

Of the greatest information security risk in the college in which data/information is easily lost, most (41.9%) of the respondents indicated that it is internet downloads. Users may download information from unsecured internet sources and this poses

security risks. This agrees with Whiteman and Mattord (2012) that unintentional errors caused by users such as downloading from unknown sources can be considered high threats to information security in an organization.

4.3.2 IT Security Awareness Pattern

Most of the respondents disagreed that there is the availability of IT security policies that are clear and easy to read (mean = 2.500, stddev = 0.76287). In certain cases, such private data and intellectual property are tightly regulated by security policies. Lack of policies might be the result of challenges such as staff variability. This is in agreement with the view of Yeo, et al.(2007) that it has been more complex bringing everybody under the security protocol/policies because of more rapidity and dynamism in Technologies that are integrating nearly everyone every day.

Also, most of the respondents disagreed that administrators in their college adhere to its IT process or security standards (mean = 2.3770, stddev = 0.71096). This agrees with Rezgui(2009) and Kandus, (2011) who also argued that although there is the availability of information security technology and official organization standards, a massive percentage of higher educational institutions do not adhere to these standards. Again, most of the respondents disagreed that the college has the level of information security they need to inspire confidence in their staff members (mean = 2.4516, stddev = 0.71695). This may be due to the lack of information security policies as asserted by Julisch(2016) that information security policy is needed to inform and inspire individuals who operate within an organization to conduct themselves properly concerning information security issues.

Furthermore, most of the respondents disagreed that higher administrators' computers in the colleges been monitored through the IT unit (mean = 2.4839, stddev = 0.78389). Experts have often stressed the focus on Continuous monitoring of the control system that is vulnerable and risk assessment from the community of IT consumers. This is contrary to the argument made by Nthala et al. (2018) that there is a need for continuous management system monitoring and risk assessment of the administrative computers. Most of the respondents also disagreed that the colleges provide them with a confidential repository for their classified data/information (mean = 2. 5323, stddev = 0.71787). This means that there is no information security in the colleges of education. Information Security is the preservation of confidentiality or protection from unauthorized use or disclosure of information. This is in agreement with de Bruijnand Janssen(2017) who defined information technology (IT) security systems in higher education as maintaining data confidentiality, ensuring data integrity, and making data available to approved users on a timely basis.

Also, most of the respondents disagreed that the colleges provide staff training to raise information security awareness (mean = 2.6129, stddev = 0.75433). Information security education, seminars, training, and awareness programs that continuously educate professionals and users, how to utilize the new and advanced security technology are indeed in dire need. This finding agrees with Kim, Mims, and Holmes (2006) who recommended that institutions should provide easily accessible security training programs for their students and staff to have effective Information Security program.

Most of the respondents again disagreed that the senior management/Administrators are actively involved in the colleges' information security issues (mean = 2.5161, stddev = 0.74089). It can be said that administrators have been ignoring information security in their administrative duties. The ignoring of information systems security by higher education administrators over the past years has caused huge data breaches and exposed a lot of confidential information. This finding contradicts that of Adu (2016) who argued that in an institution, one of the roles played by the administrators is to provide and put in place measures to ensure security in all aspects of the organization including computing infrastructure.

Lastly, most of the respondents disagreed that presentation and discussions have raised their awareness of information security attacks in their colleges (mean = 2.3548, stddev = 0.77028). This means that there are no discussions and presentations done in these colleges of education regarding information security. This has rendered the staff limited knowledge of information security. This agrees with the argument by de Bruijnand Janssen (2017) that the need for information security awareness is increasingly important due to the limited knowledge in information security issues.

4.3.3 Evaluation of present information security management system

Of the factors that that has been put in place to ensure information security in the colleges, most (30.6%) of the respondents indicated the availability of IT steering Committees in the colleges. The diverse roles of IT committees in higher educational institutions provide unique insights into the production and integration of information security awareness perspectives at the departmental and faculty level. This agrees with Nthala et al. (2018) who also state that common attacks and threats most institutions

and their employees face are operating systems vulnerabilities, malware, phishing, identity theft, and privacy violation and these are usually mitigated well in large organizations because they have IT, support team.

Also, the majority (62.9%) of the respondents said it was difficult to convince management to invest in securing a strong fortified information security network. Most managers are not so much committed to information security in their organizations. This is the same issue faced by the colleges of educations. Because of the lack of commitment on the part of the management, it is difficult to convince them to invest in information security in the colleges of education. This agrees with Moon et al.(2018) who also argued that information security has become one of the basic operational requirements of any type of organization and therefore requires the commitment of management to carry it out.

CHAPTER FIVE

SUMMARY, CONCLUSION, AND RECOMMENDATIONS

5.1 Introduction

This chapter presents a summary of the major findings of the study, conclusions and recommendations based on the findings. The presentation is done according to the study objectives.

5.2 Summary

The study found that the operating system of administrators is updated at least once a month. Also, it was found that anti-virus software is installed on the colleges' computers. Again, it was revealed that the IT staff are responsible for installing and maintaining security software on the computers in the college. Furthermore, the study revealed that the college network is secure.

The study further revealed that there is lack of IT security policies that are clear and easy to read. Also, the administrators in the colleges do not adhere to its IT process or security standards. Also, the colleges do not provide staff training to raise information security awareness. Again, the senior management/Administrators are not actively involved in the colleges' information security issues.

The study also revealed that the availability of IT steering committee is one of the factors that that have been put in place by the Colleges of Education to ensure information security. However, it was difficult to convince management to invest in securing a strong fortified information security network.

5.3 Conclusion

The study therefore concludes that the operating system of administrators is updated at least once a month. Also, it was found that anti-virus software is installed on the colleges' computers. Again, it was revealed that the IT staff are responsible for installing and maintaining security software on the computers in the college. Furthermore, the study revealed that the college network is secure.

The study further concludes that there is lack of IT security policies that are clear and easy to read. Also, the administrators in the colleges do not adhere to its IT process or security standards. Also, the colleges do not provide staff training to raise information security awareness. Again, the senior management/Administrators are not actively involved in the colleges' information security issues.

Lastly, the study concludes that the availability of IT steering committee is one of the factors that that have been put in place by the Colleges of Education to ensure information security. However, it was difficult to convince management to invest in securing a strong fortified information security network.

5.4 Recommendations

Based on the findings of the study, the following recommendations are made:

- The colleges should organise training on information security for all staff to equip them with the required knowledge to manage information in the colleges.
- There should be a regular evaluation of the information security systems of the colleges of education. This evaluation process must be dynamic and should be updated regularly to ascertain the needs and behaviour of employees and new users regularly according to the organizational vision, pattern, economy, value, and aspirations as well as objectives.

- The colleges of education need to create a framework for dealing with multidisciplinary IT security threats.
- There should be a regular evaluation of IT practice, including an awareness program, IT users' and stakeholders' motivation, and the ability to incorporate rapid changes in IT security measures.
- For all of their employees, the colleges must emphasize personal development through training, recruitment of IT consultants and technicians, certification courses, accepting only qualified IT experts. As a result, they will be able to strike a balance between their needs and organizational capabilities, potentially leading to a more secure IT management system.
- Encourage a bottom-up network architecture. For security reasons, both colleges of education recommend that participation be as broad as possible. Because of the participatory nature of IT security policy adaptation and execution requirements in both colleges, communicate problems rather than face them.
- Future studies should focus on the IT human resource and infrastructural strengths of the colleges of education.
- The study can also be replicated in other high educational institutions in Ghana to come out with the true nature of information security in the higher educational institutions in the country.

REFERENCES

Africa Cyber Report (2016). *Achieving Cyber Security Resilience*: Enhancing Visibility and Increasing Awareness. Available at: www.serianu.com (accessed on 5 January 2020).

Almeida F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European Journal of Education Studies*, 3(9).

Andale, B. (2015). *Probability Sampling*: Definition, Types, Advantages and Disadvantages. Statistics How To. Retrieved from http://www.statisticshowto.com/probability-sampling/.

Andresen, M.A., Jenion, G.W., & Reid, A.A. (2012). An evaluation of ambient population estimates for use in crime analysis. Crime Mapping*: A Journal of Research and Practice*, *4*(1), 7 – 30.

Arafat, M. J. &Daiyan, G.M. (2012). "Emergence of robust information security management structure around the world with structure around the world-wide higher education in higher education institutions: Institutions: a multifaceted security solution multifaceted security solution multifaceted security solution," *IJCSI*, vol. 9.

Cherdantseva, Y. & Hilton, J. (2013). "A reference model of information assurance & amp; security," in Availability, Reliability, and Security (ARES), 2013 Eighth International Conference on, 546–555, IEEE.

Choi, S., Martins, J.T. & Bernik, I. (2018) "Information security: listening to the perspective of organizational insiders". *Journal of Information Science, 44*(6), 752-767.

Clarke, S. (2016). "Reducing the impact of cyberthreats with robust data governance", *Computer Fraud & Security,* (7), 12-15.

Colwill, C. (2017). "Human factors in information security: The insider threat–who can you trust these days?" *Information Security Technical Report, 14*(4), 186–196.

Cram, W.A., D'Arcy, J. & Proudfoot, J.G. (2019). "Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance", *MIS Quarterly, 43*(2), 274-288.

Dahler-Larsen, P. (2011). "*The evaluation society*". Stanford University Press.

Dark, M., Epstein, R., Morales, L., Countermine, T., Yuan, Q., Ali, M., Rose, M. & Harter, N. (2006). "A framework for information security ethics education," in *10th Colloquium for Information Systems Security Education-University of Maryland, 4,* 109–115.

De Bruijn, H. & Janssen, M. (2017). "Building Cybersecurity Awareness: The need for evidence-based framing strategies". *Government Information Quarterly*, *34*(1).1-7.

Fal (2010). "Standardization in information security management," *Cybernetics and Systems Analysis, 46,* 512–515.

Garcia, G.S.C. 2006. The mother – child nexus: knowledge and valuation of wild food plants in Wayanad, Western Ghats, India. *Journal of Ethnobiology and Ethnomedicine* 2:39.

Gulappagol, L. & ShivaKumar, K.B. (2017). "Secured data transmission using knight and LSB technique", *2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques* (ICEECCOT), 253-259.

Hanus, B., Windsor, J.C. & Wu, Y. (2018). "Definition and multidimensionality of security awareness: close encounters of the second order", ACM SIGMIS Database: *The DATABASE for Advances in Information Systems, 49,* 103-133.

Ho, S.M., Kaarst-Brown, M. & Benbasat, I. (2018), "Trustworthiness attribution: an inquiry into insider threat detection." *Journal of the Association for Information Science and Technology,* 69(2), 271-280.

International Telecommunication Union (2016). *ICT Development Index 2016*. Available at: www.itu.int/net4/ITU/2016/ (Accessed 16 January, 2020).

Kermode, S., Taylor, B. & Roberts, K. (2006). "*Research in nursing and health care*: Creating evidence for practice."

Kim, H.L., Choi, H.S. & Han, J. (2019). "Leader power and employees' information security policy compliance", *Security Journal,* 32(4), 391-409.

Kofi, K. A. & Emmanuel, A. (2018). "*The phenomenon of data loss and cybersecurity issues in Ghana".*

Kvavik, R. B. & Voloudakis, J. (2003). "*Information technology security: Governance, strategy, and practice in higher education".* Educause.

Lewis, J.L. & S.R.J. Sheppard (2006). Culture and communication: can landscape visualization improve forest management consultation with indigenous communities? *Landscape and Urban Planning 77*: 291–313.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. & Pattinson, M. (2017). "Individual differences and information security awareness."*Computers in Human Behaviour, 69,* 151-156.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. & Pattinson, M. (2017). "Individual differences and information security awareness", *Computers in Human Behaviour, 69,* 151-156.

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, *9*(1), 23–41. https://doi.org/10.1080/15332861.2010.487415.

Mertens, D. M. (2007). "Transformative paradigm mixed methods and social justice," *Journal of Mixed Methods Research, 1*(3), 212–225.

Moon, Y.J., Choi, M. & Armstrong, D.J. (2018). "The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations", *International Journal of Information Management, 40*, 54-66.

Norman G. (2010). Likert scales, levels of measurement and the ''laws'' of statistics. *Adv Health Sci Educ Theory Pract*.; 15(5):625–632.

Pastor, V., Díaz, G., & Castro, M. (2010). State-of-the-art simulation systems for information security education, training and awareness. 2010 IEEE Education Engineering Conference, EDUCON 2010, 1907–1916. https://doi.org/10.1109/EDUCON.2010.5492435

Pawlowski, S.D. & Jung, Y. (2019). "Social representations of cybersecurity by university students and implications for instructional design", *Journal of Information Systems Education, 26*(4), 281-294.

Raneem, A. & Jorge, T. M. (2020). "*Information security awareness in a developing country context: insights from the government sector in Saudi Arabia*".

Safa, N.S., Von Solms, R. & Futcher, L. (2016). *"*Human aspects of information security in organizations"*, Computer Fraud and Security, 2,* 15-18.

Sebescen, N. &Vitak, J. (2017). "Securing the human: employee security vulnerability risk in organizational settings." *Journal of the Association for Information Science and Technology, 68*(9), 2237-2247.

Sekaran, U. &Bougie, R. (2010). "*Research methods for business: A skill-building approach*."

Singh, R., Keil, M. & Kasi, V. (2009). "Identifying and overcoming the challenges of implementing a project management office," *European Journal of Information Systems,* 18(5), 409–427.

Soomro, Z.A., Shah, M.H. & Ahmed, J. (2016). "Information security management needs more holistic approach: a literature review", *International Journal of Information Management, 36*(2), 215-225.

Staley, D. J. & Trinkle, D. A. (2011). "The changing landscape of higher education."*Educause Review,* 46(1), 16–33.

Ward, D. & Hawkins, B. L. (2003). "*Presidential Leadership for Information Technology., Presidency*", *6*(2) 1–11.

APPENDIX

QUESTIONNAIRE

PURPOSE OF THIS STUDY

The purpose of this research is to assess or investigate the impact of Higher Education Administrators roles in strengthening the educational and institutional information security system in Colleges of Education in the Bono Region of Ghana.

Your responses to this survey will be strictly confidential and it is mainly for academic purposes.

INSTRUCTION

Please indicate your response to the following questions by selecting the appropriate response in the spaces provided.

Organizational Information

1. Gender

   Male [ ] Female [ ]

2. Educational Background

   First Degree [ ] Med/Msc/Mphil [ ] PhD [ ]

3. Which department do you belong to?

   i. Administration [ ]

   ii. Finance [ ]

   iii. Library [ ]

   iv. Tutor [ ]

4. How many staff does your College I T department have?

   1-2 [ ] 3-5 [ ] 6-10 [ ] >15 [ ]

Information Security Practice and Technologies

5. Does your College have a dedicated department responsible for information/network security?

   i. Yes, the college has a dedicated department [ ]

   ii. Yes, but as part of another department (I T department) [ ]

   iii. No [ ]

6. How often does the College update the Operating System (Windows) of administrators

   i. Set to update automatically [ ]

   ii. At least twice a week [ ]

   iii. At least once a month [ ]

   iv. Never [ ]

7. Do you have anti-virus software installed on the College's computers?

   Yes[ ] No [ ] Don't know [ ]

8. Who is responsible for installing and maintaining security software on your computers in your college?

   Administrator [ ] I T Staff [ ] Other Staff [ ]

9. How secure do you think your college network is?

   Very Secure[ ] Secure [ ] Not Secure [ ] Don't know [ ]

10. Which security measures have your college implemented?

    Intrusion Detection system[ ] File encryption [ ] Antivirus Others [ ]

11. What do you consider to be your greatest information security risk in your college in which data/information is easily lost to

    Incorrect Configuration [ ]

    Internet downloads [ ]

    Email viruses [ ]

    Others [ ]

I T Security Awareness Pattern

12. My College has I T security policies that are clear and easy to read

    Strongly Agree [ ]

    Agree [ ]

    Strongly Disagree [ ]

    Disagree [ ]

13. Administrators in my college adhere to its I T process or security standards

    Strongly Agree [ ]

    Agree [ ]

    Strongly Disagree [ ]

    Disagree [ ]

14. My College has the level of information security we need to inspire confidence in our staff members

    Strongly Agree [ ]

    Agree [ ]

    Strongly Disagree [ ]

    Disagree [ ]

15. Higher administrators' computers in my college been monitored through the IT UNIT

    Strongly Agree [ ]

    Agree [ ]

    Strongly Disagree [ ]

    Disagree [ ]

16. My College provides me with a confidential repository for our classified data/information (Administrative & Academic data)

    Strongly Agree [ ]

    Agree [ ]

    Strongly Disagree [ ]

    Disagree [ ]

17. I know exactly where to go in my college when I need information security to expect concerning data storage.

    Strongly Agree [ ]

    Agree [ ]

    Strongly Disagree [ ]

    Disagree [ ]

18. My College provides staff training to raise information security awareness

    Strongly Agree [ ]

    Agree [ ]

    Strongly Disagree [ ]

    Disagree [ ]

19. My College adhere to I T process or security frameworks and or standards

    Strongly Agree [ ]

    Agree [ ]

    Strongly Disagree [ ]

    Disagree [ ]

20. My College has the level of information security we need to inspire confidence in our staff members

    Strongly Agree [ ]

    Agree [ ]

    Strongly Disagree [ ]

    Disagree [ ]

21. Senior management/ Administrators are actively involved in our college's information security issues.

    Strongly Agree [ ]

    Agree [ ]

    Strongly Disagree [ ]

    Disagree [ ]

22. Presentation &discussions have raised my awareness of information security attacks in my college.

    Strongly Agree [ ]

    Agree [ ]

    Strongly Disagree [ ]

    Disagree [ ]

Evaluation of present information security management system

23. What do you think will help improve your colleges' information security levels?

    I T steering Committees [ ]

    Better staff information security awareness [ ]

    Advanced security technology [ ]

    Others [ ]

24. How difficult is it in your opinion to convince management to invest in securing a strong fortified information security network?

    Very easy [ ] Easy [ ] Very Difficult Difficult

25. What do you think will help improve your colleges' information security levels?

    ……

    ……

26. Do you have any other comments, questions, or concerns regarding information security in your College?

    ……

    ……