AKENTEN APPIAH-MENKA UNIVERSITY OF SKILLS TRAINING AND ENTREPRENEURIAL DEVELOPMENT

INFORMATION SECURITY POLICY COMPLIANCE, WORKERS' PERCEPTIONS, MOTIVATION AND BREACHING EFFECTS ON ORGANIZATION'S REVENUE.

FRANCISCA OWUSUWAA ANTWI

MASTER OF SCIENCE DISSERTATION

2022

AKENTEN APPIAH-MENKA UNIVERSITY OF SKILLS TRAINING AND ENTREPRENEURIAL DEVELOPMENT

INFORMATION SECURITY POLICY COMPLIANCE, WORKERS' PERCEPTIONS, MOTIVATION AND BREACHING EFFECTS ON ORGANIZATION'S REVENUE.

FRANCISCA OWUSUWAA ANTWI

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 Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development

JULY, 2022

DECLARATION

STUDENT'S DECLARATION

I, **Francisca Owusuwaa Antwi**, declare that this dissertation, with the exception of quotations and references contained in published works which have all been identified and duly acknowledged, is entirely my own 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 Akenten Appiah-Menka University of Skills Training and Entrepreneural Development.

DR. JOSHUA DAGADU

SIGNATURE:…….

DATE:…….

DEDICATION

To my dad, Mr. Antwi-Mensah Peter, my daughter, Mutilina Nana Agyemang Acheampong, and my husband, Mr. Acheampong Francis.

ACKNOWLEDGEMENTS

I would like to express my profound gratitude to Dr. Dagadu Joshua (Department of Information Technology Education, AA-MUSTED) for his support, mentoring, guidance and patience towards me and throughout this work.

I am also grateful to my dad, Mr. Antwi-Mensah Peter, my daughter, Mutilina Nana Agyemang Acheampong, and my husband, Mr. Acheampong Francis, and Rev. Father Francis Opoku for their encouragement and prayer during this period.

Finally, I would like to thank my study partners, Mr. Barfi Adomako Andrews and Mr. Nkansah James for their massive support.

TABLE OF CONTENTS

CONTENT	PAGE
DECLARATION	iii
DEDICATION	iv
ACKNOWLEDGEMENTS	v
TABLE OF CONTENTS	vi
LIST OF TABLES	ix
ABSTRACT	x
CHAPTER ONE: INTRODUCTION	**1**
1.1 Background	1
1.2 Problem Statement	4
1.3 Aim of the Study	5
1.4 Objectives	5
1.5 The Research Questions	6
1.6. Significance of the study	6
1.7 Delimitation of the Study	6
1.8 Limitation of the Study	7
1.9 The Research Approach	7
1.10 Theoretical Perspective	7
CHAPTER TWO: LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT	**8**
2.1 Introduction	8
2.2 Workers' perceptions about the need for information security policy compliance	8

2.3 Factors that motivate compliance with information security policy compliance 13

2.4 Effects of information security breaches on revenue 21

CHAPTER THREE: METHODOLOGY 28

3.1 Introduction 28

3.2 Research Design Process 28

3.2.1. Information Security Policy Compliance 29

3.2.2. Factors that Influence Information Security Policy Compliance 29

3.2.3. Information Security Breaches on Revenue 29

3.3 Population and Sampling procedure 30

3.4 Data collection 30

3.5 Data Analysis Technique 31

3.6 Validity and Reliability 32

3.7 Ethical Consideration 32

CHAPTER FOUR: PRESENTATION OF RESULTS AND DISCUSSION 33

4.1 Introduction 33

4.2 Presentation of Results 33

4.2.1 Demographies 33

4.2.2 Q1: What are the workers' perceptions about the need for compliance with 35

4.2.1 Q2: What are the factors that motivate employees of an organization to 38

4.2.3 Q3: To what extent do information security breaches affect an organization's 42

4.3 Discussion of Results 45

4.3.1 Perceived importance of Information security policy compliance 45

4.3.2 Factors that motivate employees to comply with Information Security 46

4.3.3 Effects of Security Breaches on Revenue 47

CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS **48**

5.1 Conclusion 48

5.2 Recommendations 48

REFERENCES **50**

APPENDICES **64**

LIST OF TABLES

TABLE	PAGE
Table 3.1: Reliability Statistics of Constructs	32
Table 4.1: Respondents' Gender	33
Table 4.2: Respondents' Age Distribution	34
Table 4.3: Respondents' Company	34
Table 4.4: Respondents' Department	35
Table 4.5: Respondents' Work Experience	35
Table 4.6: Customers' perceived importance of ISP compliance	37
Table 4.7: Factors that Motivate Employees' Compliance	40
Table 4.8: Effects of ISP Breaches on Organizations' Revenue	44

ABSTRACT

It is generally conceived that the security of an organization's information resources largely depends on compliance with the organization's information security policies. Thus, this research investigates the employees' perception of the importance of information security policy compliance, the factors that motivate them to comply with the policies, and the effects of the policy breaches on the organization's revenue. A descriptive quantitative method was used to collect and analyze data from four different companies in the Ashanti region of Ghana, West Africa. The findings showed that information security policy compliance is very significant to ensuring the integrity, confidentiality, and availability of the information resources of an organization. Also, both intrinsic and extrinsic motivations influence employees to comply with security policies. The direct effects of security breaches on revenue were not ascertained however, the employees believed that it has effects on the capital growth of organizations. The study has placed much emphasis on the need for organizations to enforce compliance with information security policies.

CHAPTER ONE

INTRODUCTION

1.1 Background

Security policy is the foundation of any security regime and specifies the strategies behind an organization's information security approach by a written document, directly linked to the overall policies of the organization (Fulford & Doherty, 2003; Höne & Eloff, 2002). The effective security of the entire information resources of an organization is anchored on the formulation of an easyto-understand, systematically designed policy that is fully integrated into the organization. Again, it is postulated that one increasingly important mechanism for protecting corporate information, and in so doing reducing the occurrence of security breaches, is through the formulation and application of a formal information security (Hinde, 2002; Vroom & Von Solms, 2004). This is because employees are often resistant to security policies (Hu et al., 2007) and bypass them. This exposes their organizations to data loss and cybercrime (Dhillon, 2001).

The mechanisms employed by managers to enforce information security policies are categorized into those that are external to the end-user and those that stem from the users' perceptions and belief systems. One of the chief strategies employed by organizations to ensure the security of information resources is the establishment of comprehensive information security policies and their compliance. When employees comply with the information security requirements, the probability of security breaches tends to drop significantly (Al-omari & El-gayar, 2012). Also, it is postulated that every effort and financial resources could be injected into establishing information security policies and procedures but this will amount to nothing if employees do not show

commitment to comply with them (Herath & Rao, 2009). This is because, in organizations where employees become so careless in handling information security procedures and policies, the organization loses billions of dollars which tends to weaken its financial strength (Privacyrights.org, 2006). Breach such as denial-of-service attack has the potency to cripple a company's sales for a considerable period as it happened to Yahoo and eBay. This form of attack weakens customers' trust and confidence which is likely to make them withdraw themselves from doing business with the breached company (Niccolai, 2000; Yayla & Hu, 2011).

Empirical evidence has shown that despite the strategies and resources put in place to ensure employees compliance, the issue is still a challenge because employees intentionally breach security policies to expediently get their job done (Bedford, 2008). This has propelled many researchers to investigate the human and organizational factors that motivate employees to comply with information security procedures and requirements (Bulgurcu et al., 2010; D'Arcy et al., 2009; Kraemer, Carayon & Clem, 2009; & Siponen, 2010). The time and energies channeled into the information security policies and their compliance is worth it because information security breaches come with a huge cost especially to ecommerce firms. And it should be noted that these breaches and their severity are on the ascendency (Yayla & Hu, 2011). Businesses lose billions of dollars every year due to the attacks that are launched against the information resources of the breached companies (Cavusoglu, H., Mishra, B. and Raghunathan, 2005; Gordon, Loeb, Lucyshyn & Richardson, 2004; Niccolai, 2000). This negative phenomenon has awakened researchers to search out and also propound theories, and expound empirical studies about the effective means of mitigating this canker. These theories are formulated based on different perspectives of researchers. Some of the

theories reviewed by this study are to justify that the greater part of the research on employees' compliance focus on the behavior, attitude, habit, perception, and probably environmental factors such as deterrence (Herath & Rao, 2009). These theories include: Rational Choice Theory (RCT) that deals with employees' belief system towards information security compliance (Bulgurcu et al., 2010). Protection Motivation Theory (PMT) (Herath & Rao, 2009). This theory hinges on the premise that a lot of information breaches occur in organizations due to a lack of motivation and insecurity among employees towards compliance with information security policies (Albrechtsen, 2007). The insecurity arises out of the perceived dangers that are associated with adherence to information security procedures (Axelrod & Newton, 1991). The General Deterrence Theory (GDT) (Iolations & Vance, 2010). This theory stresses that the intensity of punishment and other severe deterrent measures can compel employees to comply with information security policies (Herath & Rao, 2009; Straub, 1990; Straub & Welke, 1998).

On the contrary, it is posited by (Boss et al., 2009) that to win employees' hearts towards compliance with the information security policies, rewards should be used. Perceived Ease of Use of ISP (PEOU) and Perceived Usefulness of Protection (PUOP). The PEOU and PUOP theories use as a basis the Technology Acceptance Model (TAM) (Dinev et al., 2009). These theories focus attention on employees' behavior, attitude, habits, and perceptions towards information security policy compliance (Dinev et al., 2009; Rhee, Kim & Ryu, 2009). The theories go on to explain that employees exhibit greater willingness to comply with information security policies when they realize that doing so comes a bit easier and will also make them perform better (Al-omari & El-gayar, 2012). The Theory of Planned Behavior (TPB) and the Theory of Reasoned

Action (TRA) (Ajzen & Fishbein, 1975) were also reviewed to project that employees' attitude, intentions, and behavior are major factors that influence their compliance with information security policies (Pahnila et al., 2007). This study is thus conducted to assess the contribution of compliance with the information security policies to the growth of an organization in terms of revenue mobilization. This will inform researchers and managers whether compliance with information security policies' effect on building capital can be a strong motivating factor for information security policy compliance.

1.2 Problem Statement

Despite an attempt by many organizations to formulate and enforce information security policies, it is revealed that these policies fail to impact the users on the ground (Höne & Eloff, 2002). Included in its failure is the lack of compliance with these policies by employees. This has triggered a lot of research in the area of information security policy compliance and empirical evidence shows that more research still needs to be conducted in this area (Herath & Rao, 2009).

This study is motivated by the fact that compliance with information security policies and procedures is traditionally not a part of merit-pay schemes that assess an organization's performance (Boss et al., 2009). It, therefore, seeks to examine the impact of information security policy compliance on the capital growth of organizations as a factor for employees' compliance with information security policies. The next section deals with the various empirical studies and the theories that were reviewed to trumpet the importance of information security policy compliance, the factors that influence information security policy compliance, and the effects of information

security policy breaches on the breached organization. The theories reviewed served as the premise for the formulation of the hypotheses of the study. The various methods employed to sample participants, collect data and analyze it to conclude also follow in the third section. Section four of the study deals with the analysis and implications of the study. The last section discusses the interpretation of findings, conclusions, and recommendations based on the findings.

1.3 Aim of the Study

This study aims to critically examine the relationship between information security policy compliance and the achievement of organizations' aims in terms of capital growth. It seeks to find out if the contribution of compliance with the information security policy to organizations' capital growth can be a strong factor in the array of reasons for information security policy compliance.

1.4 Objectives

The following are the main objectives of this study.

i. To determine workers' perceptions about the importance of information security policy compliance.
ii. To identify the factors that motivate compliance with information security policies in an organization.
iii. To identify the effects of information security policy breaches on an organization's revenue.

1.5 The Research Questions

The study seeks to investigate the following research questions

1. What are the workers' perceptions about the need for compliance with information security policy in organizations?
2. What are the factors that motivate employees of an organization to comply with information security policies?
3. To what extent does information security breaches affect an organization's revenue?

1.6. Significance of the Study

This study is meant to draw researchers' attention to the influence of information security policy compliance on an organization's capital growth as a major factor that can motivate employees to comply with information security policies.

1.7 Delimitation of the Study

The scope of this study will be in the Ashanti region of Ghana and it will include both public and private organizations. One manufacturing company and one wholesale company in Kumasi will be considered. 10 respondents will be selected from each of these companies using a random digit table. Information security policy compliance has many components but this study is limited to its contributions towards the capital growth of these organizations. As such a survey method, consisting of questionnaires will be employed.

1.8 Limitation of the Study

The major foreseen challenge of the study is getting the organizations selected for the study to trust the researcher with the confidentiality of their information. Also, time will not allow the researcher to include many organizations within the selected region which could have made the study representative enough for nationwide generalization.

1.9 The Research Approach

The researcher adopts quantitative means and procedures, as defined by (Baxter & Jack, 2008) to conduct the study. This approach was chosen over the qualitative approach because the study seeks to validate, refine or ignore several hypotheses that the researcher has proposed. More so, the study seeks to find the relationship between the various variables and how one affects the other. The analysis will thus be done in numerical form.

1.10 Theoretical Perspective

This study will adopt the systems approach of organizational theory. This is because the researcher believes that there is an interaction between all the faculties of an organization. Therefore, the success of every organization is the product of the functions of its interlocked departments namely, information systems, the people, structure, and the organization's physical settings and the environment. The researcher sees this perspective as desirable because information security policies and their compliance is not independent of the other factors of the organization. As a policy, it forms an integral part of organizations and affects every unit of them.

CHAPTER TWO

LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

2.1 Introduction

This chapter reviews some of the related studies done by researchers in the field of information security policy compliance. The index words used to search for the literature are the variables of this study. Online databases such as Google Scholar, Science Direct, and Elsevier were mostly accessed for the literature needed. To give a comprehensive picture of literature, the literature search encompasses published research from the last two decades, with a focus on studies released as recently as feasible. Major theories on information security policy compliance, especially on the factors that influence security compliance are discussed in this chapter. Also, the chapter reviews most of the empirical shreds of evidence that relate to the importance of information security policy compliance and the adverse effects of security breaches on companies. The theories reviewed in this section served as the basis for the formulation of the hypotheses of the study.

2.2 Workers' Perceptions about the need for Information Security Policy Compliance

The broad aim of the information security policy is to provide the "ideal operating environment" for the management of information security (Barnard et al., 1999). This is achieved by defining "the broad boundaries of information security" as well as the "responsibilities of information resource users" (Hone & Eloff, 2002b, p. 145). More specifically, a good security policy "outline individual responsibilities, define authorized and unauthorized uses of the systems, provide venues for employee

reporting of identified or suspected threats to the system, define penalties for violations, and provide a mechanism for updating the policy" (Whitman, 2004, p. 52). While the Information security policy provides the framework for facilitating the prevention, detection, and response to security breaches, the policy document typically is supported by standards that tend to have a more technical or operational focus (Dhillon, 2001). As (Hinde, 2002) put it, the information security policy is now the sine qua non (indispensable condition) of effective information security management. In a similar vein, (Solms et al., 2011) note that the information security policy is the heart and basis of successful security management. Despite this, it's important to remember that successful policy design does not always imply the security of an organization's information resources. It takes methods to ensure that information security policy is followed to achieve the desired results. Employees' compliance with Information Security Policies is critical to the success of an information security program.(Al-omari & Elgayar, 2012).

This is because it is asserted that Information security in an organization largely depends on employee compliance with its policy (Yazdanmehr et al., 2020). Effective information security management and security culture rely on employees complying with security policies and this has given the rise to many organizations trying to influence employees' security behavior to comply with security policy (Beautement et al., 2008). Information security compliance is therefore needed to achieve the confidentiality, integrity, and availability of information resources of every organization (Amankwa et al., 2018). Compliance with information security policies cannot be overemphasized because when individuals choose to disregard security policies and procedures, the organization is at risk (Boss et al., 2009). The level of

compliance, additionally, can signal to management that the information security policies of the organization have been effectively implemented. So, if employees tend to disregard the presence of the information security policy, then it shows, to some extent that it has not met their goodwill. (Boss et al., 2009). The fatal mistake any organization can make is to assume that just informing employees about the presence and benefit of information security policy will make them comply with it. This explains why compliance with information security policies is intensively enforced on the premise that a large number of security breaches involve internal employee negligence and insider breach. (Chen et al., 2016). Employees must therefore be encouraged to go to whatever extent possible to comply with information security requirements and procedures because the cost of recovering from security breach far exceeds any cost of compliance measures (CSC, 2019).

Generally, to ensure the successful functioning of an organization, employees must adhere to the policies of the organization (WEITZ et al., 2008). It is also ascertained that the key threat to information security in an organization is noncompliance on the part of employees because they are considered as the weakest link in any system. (Pahnila et al., 2007). When employees refuse to comply with the information security requirements, it places the organization's assets and business in danger (Hair, Black, Babin, Anderson, Tatham, 2006). It makes the organization so vulnerable that the confidentiality, integrity, and availability of its crucial information cannot be guaranteed. In this information and technology age, any organization that makes the security of its information resource a core mandate is considered a learning organization. This is because learning organizations adhere to good business practices and procedures (Gladwell, 2013). The long-term effect is that they can preserve their

competitiveness even in a changing business environment (Desai, 2020). In very simple but clear terms, (Pahnila et al., 2007) asserted that to mitigate information security breaches, employees must adhere to its compliance. Adherence to the information security protocols and procedures makes the organization formidable against intrusion mechanisms by unauthorized personnel. Given its adverse effects on an organization's information resources, noncompliance with information security requirements has become a major concern for technology security managers (Vance, 2010). Compliance with information security requirements on the other hand, in no doubt, helps to mitigate the risk of information breaches in an organization (Cheng et al., 2013; Ifinedo, 2014). These security breaches with their severe economic consequences are assuaged best when employees comply with information security policies and procedures (Anders, 2000).

Also, compliance with the information security policies earns the organization strong goodwill from its customers. This increases the organization's revenue because it is established that organizations that do not have proper information security policies compliance management are likely to experience breaches that tend to weaken the revenue base of the organization (Yayla & Hu, 2011). Effective compliance measures minimize the degree of risk of damages in the event of an attack on the information resources of a firm (Deane et al., 2019). Organizations' operational setbacks that attend to information security breaches are avoided when there are structured measures to ensure compliance with the information security policies (Ligato, 2015). It should be noted also that if information resources are not protected through strategic measures of policies and their compliance, not only organizations suffer, but the entire country (Volz, 2016). An organization with a firm compliance culture has a strong competitive

advantage and position because they gain goodwill among customers (Deane et al., 2019) whereas those without any strategic measures to enforce compliance have reputational damage (Desai, 2020). Moreover, information security compliance enforcements, unlike post-attack measures, save the organizations much energy, time, and money in trying to find the cause of an attack, means of amendments, and formulation of countermeasures (Campbell et al., 2003). Customers also consider companies with a strong compliance culture to be less risky and hence more desirable (Deane et al., 2019). The researchers then assert that this considerably reduces the concerns about the security compromise that negatively affects a business's principal source of revenue.

In conclusion, It is important to adopt technology as a tool to fight information breaches in an organization but as noted by (Herath & Rao, 2009), technological tools are not adequate in terms of safeguarding corporate data. Employees' behavior has grown increasingly important, and it's difficult to predict it, especially when research has revealed that end users have differing perspectives on security (Desai, 2020). This, therefore, calls for intensive measures and mechanisms to ensure that they adhere to every security protocol established by the organization. This is because research has shown that noncompliance with information security policies by employees appears to be the biggest cause of security issues, costing businesses millions of dollars (Herath & Rao, 2009). When employees are committed to adherence to the information security policies of an organization, the dilemma of security breaches is utterly minimized (Desai, 2020).

Hypothesis 1: ***Information security policy compliance is very necessary for the security of the information resources of every organization.***

2.3 Factors that Motivate Compliance with Information Security Policy Compliance

Identifying the factors that motivate employees' compliance with their organization's Information Security Policy is an important step toward helping information security managers understand and solve behavioral and managerial issues in information security management. Based on the analysis of the extant literature, it is evident that existing theoretical developments have been effective in defining the factors that enhance compliance or prevent system abuse. (Al-omari & El-gayar, 2012).

Both internal and external strategies have been adopted to motivate employees' information security policy compliance. However, it is noticed that almost all the theories and empirical evidence available focus on the employee as a link in the information security policy system. Because the above, employees complied with information security policies have been studied from diverse angles with different models and theories. Compliance-related beliefs derived from the theory of Rational Choice were employed to explain employees' attitudes towards information security compliance (Bulgurcu et al., 2010). Another study also employed Protection-Motivation Theory (PMT), General Deterrence Theory (GDT), and organizational behavior to investigate the motivational factors rooted in the adoption of information security policies and practices. (Herath & Rao, 2009). The GDT establishes its claims on the premise that as punishment certainty and severity increase, unwanted behaviors can be deterred (Herath & Rao, 2009; Straub, 1990; Straub & Welke, 1998). This fact

was echoed in another study to establish that punishment may serve to uphold social norms within an organization, signal appropriate and inappropriate behaviors to employees, and deter deviant acts (Trevino, 1992). Inherent in punishment is an element of fear which is also a positive predictor of a user's behavioral intention to comply with recommended individual security acts (Johnston & Warkentin, 2010). Again, another study has also found that the severity of the penalty affects employees' intention to comply with Information Security Policies (Herath & Rao, 2009). Employees tend to increase their intention to comply with information security policies when abuse or noncompliance attracts punishment especially when there is an increase in the perceived certainty and perceived severity of punishment (Chen et al., 2015). The certainty denotes that an employee becomes aware that his/her negative deeds will be found out and severity means those deeds will be harshly punished. There is also the certainty that the punishment will occur quickly (Pahnila et al., 2007).

Moreover, when an organization's deterrent mechanisms (especially the application of punishment) are geared towards information security breaches, it results in significantly lower computer abuse (Straub, 1990). It is thus conclusive that punishment as a deterrent strategy can result in positive outcomes (Chen et al., 2015) because it sends signals to employees that noncompliance comes with a cost (Bulgurcu et al., 2010). Objections have also been raised against punishment as an effective method to cajole employees to comply with Information security policies. For instance, most of the organizational theorists vouch for positive enforcement strategy—reward, claiming that reward provides needed incentive and motivation for compliance (Boss et al., 2009) and gives a thumb up to employees that the organization's expectations are being met (Boss et al., 2009; Eisenhardt, 2008). It also signals to employees that compliance with

the information security policies is mandatory (Boss et al., 2009). It was further argued that punishment is not a high priority choice for managerial application because the presumed negative consequences may outweigh any benefits it renders (Sims, 1980). It is also revealed that greater deterrent effort appears to contribute to better Information security effectiveness even though enforcing more severe penalties does not seem to prevent Information Security abuses (Kankanhalli et al., 2003). In support, (Pahnila et al., 2007) found that sanctions do not affect employees' intentions to comply with Information Security Policies.

Instead of punishment, it is beneficial to employ reward because it tends to influence employees' performance and compliance with the organization's policies (Sims, 1980). This is because no matter how clear security policies are stated and the seriousness an organization attaches to compliance, without reward, compliance to the security policies will be poor (Boss et al., 2009; Eisenhardt, 2008). Proper use of rewards as a means to control and manage employees' behaviors motivate the employees, promote excellence, attract and retain talent and increase job satisfaction (D'Arcy et al., 2009; Zenger, 1992). For a better control mechanism to ensure compliance with information security policies, the reward is recommended (Chen et al., 2015). It is posited that when employees are faced with making a rational choice between compliance and noncompliance, the reward becomes an influencing factor (Bulgurcu et al., 2010).

This notwithstanding, it is argued that rewards are not so effective because it makes employees focus on their interest instead of the organization's goals (Bloom & Milkovich, 2017). However, it is worthy to note that in whatever way(s) one looks at it from, it is recommended that deterrent strategies are employed against undesirable

behavior such as computer abuse and noncompliance with security policy (Chen et al., 2015). In conclusion, both reward and punishment can be employed by the organization to ensure compliance with information security policies because punishments interact (Andreoni et al., 2003). Moreover, individuals are motivated by self-interest and definitely will tend to respond to acts that are associated with reward and punishment (Tyler & Blader, 2005).

Drawing on the Technology Acceptance Model (Davis et al., 1989), it is posited that employees' intention to comply with the organization's information security policies is influenced by Perceived Ease of Use of information security policies (PEOU) and Perceived Usefulness of Protection (PUOP) afforded through the use of information security policies. The role of Perceived Behavioral Control (PBC) antecedents to PEOU and PUOP, namely self-efficacy and controllability, which in turn are rooted in the Theory of Planned Behavior (TPB) (Ajzen, 2002), have also been considered. Also, the role of information security awareness has been investigated and it is postulated that it will influence employees' PEOU of information security of policies and PUOP provided by the policies leading to compliance with the information security policies. It is assumed that an employee's intention to comply with the requirements of the organization's Information Security Policies is associated with the degree to which the employee believes that using ISPs' roles and responsibilities to safeguard the organization's information technology resources will enhance their job performance (PUOP) (Al-omari & El-gayar, 2012). This is partly because, as asserted by research that employees are rational self-interested actors and that a decision not to comply relies on weighing cost and gains (Akturk et al., 2015; Yazdanmehr et al., 2020) .

Other studies employed different theories to enhance employees' compliance with information security policies and reduce systems misuse. Based on the Theory of Planned Behavior (TPB), it is also postulated that higher awareness leads to higher confidence (Dinev et al., 2009) in preventing negative technologies (such as computer viruses, spyware). Drawing on TPB and Rational Choice Theory (RCT), it was found that attitude, normative belief, and self-efficacy have a significant effect on employees' intention to comply with ISPs. This was reiterated in another study that personal values and moral beliefs are seen as self-imposed sanctions adopted by employees are very key in predicting information security policy compliance (Hsu & Lowry, 2015; Nagin & Paternoster, 1993).

The RCT was proposed on the premise that employees will weigh the cost and benefit of compliance or noncompliance with defined security policies. In this respect, the outcome of compliance or noncompliance is of much concern to employees and they are likely to opt for an action whose outcome will satisfy them (McCarthy, 2002). It should be made clear that the satisfaction sought by employees' compliance is not necessarily quantified in monetary terms (Paternoster & Pogarsky, 2009). It should again be noted that employees' behaviors play a very crucial role in dealing with information security abuse and for this, it is asserted that the breaches in information security in an organization are a result of the lack of attention paid to employees' behavior (Ifinedo, 2014). It is thus recommended that in dealing with prevailing breaches in an organization's information systems' security, employees' security behavior must be strengthened (Crossler et al., 2013).

Therefore, organizations must influence employees' behavior towards intention to comply with security policies (Amankwa et al., 2018). What influences employees most to comply with information security policies is attitude (Ifinedo, 2014; Siponen et al., 2014). This is because it was posited that when employees develop a positive attitude towards information security policy compliance, breaches in the information resources of an organization decline significantly (Parsons et al., 2014).

Also, it is believed that employees are motivated to comply with information security policies when they are convinced that the values of the organization are in line with their personal values (Kranz & Haeussinger, 2014; Malhotra et al., 2008).
Anderson and Agarwal (2010) employed Protection Motivation Theory (PMT) along with the Theory of Reasoned Action (TRA) and TPB and found that home computer users' intentions to perform security-related behavior are influenced by a combination of cognitive, social, and psychological factors (Al-omari & El-gayar, 2012).

To enforce compliance with information security policy, (Pahnila et al., 2007) found that habits have a significant effect on employees' compliance with Information Security Policies. These habits/behaviors are increased when employees feel satisfied and secured with their job (Goel & Crain, 2010). Moreover, a study conducted by (Herath & Rao, 2009) revealed that employees are likely to portray a positive attitude towards information security policies if they are convinced that compliance will positively affect the organization. It is also posited that employees seem ill motivated to comply with security policies and procedures and more often appear to follow their well-honed habits; showing unwillingness towards behavioral changes (Boss et al., 2009; Herath & Rao, 2009). As it is shown, this comes as no surprise because

individuals behave based on judgmental choice and self-reactive influences (Sommestad et al., 2014). It is also clear that employees develop an internal desire to comply with information security policies if they perceive that the policies are legitimate and value congruence (Tyler & Blader, 2005).

Employees' intention to comply with the information security policies is also influenced greatly by self-efficacy. This means that the degree to which they perceive that they have the required competence, skills, and knowledge to comply with the security policies can determine their willingness or unwillingness to adhere to the policies. Even if they have what it takes to comply with the information security policies, they still contemplate the cost and benefit of complying with the policy (Bulgurcu et al., 2010). Thus, the overall assessment of the outcome determines employees' compliance with the information security policy compliance (Ajzen & Fishbein, 1975). According to (Bulgurcu et al., 2010), the beliefs about the assessment of consequences by employees before any intention to comply with information security policy hinges on the following: (a) perceived benefit of compliance, (b) perceived cost of compliance, and (c) perceived cost of noncompliance. Interestingly, the perceived benefit of compliance summarizes the favorable outcomes in favor of employees by complying with the information security policies. In the same way, if employees' sense personal harm for noncompliance with information security policy requirements, they are influenced to comply (Tyler & Blader, 2005).

Moreover, if it is perceived that compliance will consume much time and effort, then employees will show unwillingness to comply (PricewaterhouseCoopers LLP, 2008). This is mostly because they tend to perceive that compliance will stiffen productivity (Iolations & Vance, 2010; Warkentin et al., 2004). In certain regards, information

security policy requirements don't suit employees in a sense that it clashes with their primary job demands which compel them to sacrifice compliance (Pahnila et al., 2007). Furthermore, the same study conducted by (Pahnila et al., 2007) revealed that if information security policies do not seem relevant an sufficiently up-to-date to support the organization's vision, employees will be reluctant to subscribe to its adherence. In the same vein, if employees find out that the information security policies are not reasonable (i.e., they don't suit them) they will not comply with them (Vance, 2010).

In conclusion,to address the compliance concern, different strategies for effective security policy enforcement have been proposed. Compliance-related beliefs derived from the theory of Rational Choice were employed to explain employees' attitudes towards information security compliance (Bulgurcu, et al., 2010). Another study also employed Protection-Motivation Theory (PMT), General Deterrence Theory (GDT), and organizational behavior to investigate the motivational factors rooted in the adoption of information security policies and practices. (Herath & Rao, 2009).

Also, Using the Technology Acceptance Model (Davis et al., 1989) as a basis, it is posited that employees' intention to comply with the organization's information security policies is influenced by Perceived Ease of Use of information security policies (PEOU) and Perceived Usefulness of Protection (PUOP) afforded through the use of information security policies. Moreover, The role of PBC antecedents to PEOU and PUOP, including self-efficacy and controllability, which are founded in the Theory of Planned Behavior (TPB)(Ajzen, 2002), has also been explored.

In addition to all the theories reviewed above, there is the need for senior management to show commitment and provide support for information security policy compliance. There should also be the implementation of appropriate controls to minimize or guard against risks and threats, and thorough communication of security issues to users of both information and information systems through relevant education (Fulford & Doherty, 2003).

Hypotheses 2A: *Factors that influence employees to comply with information security policies are mostly those that deal with employees' behavior/attitude and application of a stimulus.*

Hypothesis 2B: *Employees develop good intention to comply with information security policies when they perceive that the policies suit/benefit them and also contribute to something worthwhile.*

2.4 Effects of Information Security Breaches on Revenue

An information security breach is defined as a malicious attempt to interfere with a company's business and its information (Cavusoglu et al., 2014). It can take the form of denial of access, modification/distortion of information, deletion of information, or unauthorized access to information (Meznar et al., 1994). Simply, information security breaches comprise a breach of confidentiality (unauthorized users having access to restricted information), availability, also called denial of service attack (prevention of authorized users to have access to information when needed), and integrity (inconsistencies in data available to users) (Anthony, Choi, 2006; Benesh, & Clark, 1994). All these categories of information security breaches have significant effects on the market value of firms (Anthony, Choi, 2006; Ettredge, 2003).

Additionally, it can be infection of computers with a virus and a variety of other attacks. Studies have even revealed that most of the information security breaches stem from virus attacks, which normally lead to breaches of information availability and integrity (Gordon et al., 2011). However, it is noteworthy that Some data security breaches fall under two or more of the categories listed above. For instance, a breach of confidentiality will likely lead to a breach of availability when the breached firm is folded up as a result of the breach of confidentiality (Gordon et al., 2011). It should be stressed that not all forms of security breaches have the same degree of economic effect on firms (Campbell et al., 2003). This is because each type of breach comes with a diverse degree of effect on the target firm (Yayla & Hu, 2011).

However, every form of breach in the information security of an organization is a big blow to them (Cavusoglu et al., 2014) because information security breaches may result in significant financial losses for businesses (Da Veiga, & Eloff, 2010). Security breaches are well planned and orchestrated to the extent that firms that are considered as giants in this information age fall prey to them (Weill, 1992). It was reported that an attack against Microsoft prevented millions of users from accessing information resources from the web pages and robbed them of revenues from the online advertisements on some of its pages (Buckman, 2001). Another report confirmed that a denial-of-service attack against Yahoo drained the firm $500,000 in just 3 hours which nearly collapsed the firm (Kedrosky, 2000). A similar attack hit Yankee Group which drained a whopping $1.2 billion from the company (Genusa, 2001). In 2001 alone, (Power, 2002) reported that close to $ 456 million went down the drain due to information security breaches. (Wang, 2013) also reported that HTC, an electronic manufacturing firm experienced a security breach by which its confidential design

technology was sold to competitors, which resulted in a loss of the company's identity and financial gains. There are both explicit and implicit costs to firms due to information security breaches. The explicit costs include the costs of detecting and correcting such breaches. The implicit costs include loss of current and future revenues resulting from the deterioration of both the relationships between a firm and its customers and between a firm and its business partners (Iheagwara et al., 2004; Mcconnell et al., 1985; Ning et al., 2001). Also, there is a loss of "substantial shareholder value" in the event of information security breaches (Malhotra, 2010). Some of the identified costs associated with information security breaches in an organization are folding up business due to lack of trust and confidence among customers, resolving the breach, and all other licit issues that will result from the breach (Campbell et al., 2003).

It is even reported that Computer abuse is a major source of security incidents that accounts for 50 percent to 75 percent of all incidents originating from within an organization, and it causes significant financial losses to the organization (D'Arcy et al., 2009). It is also noteworthy that the effects of information security breaches in an organization go beyond the breached organization and affect the market value of the security technology firm(s) associated with the said form of the breach (Cavusoglu et al., 2014). Some press reports and survey results suggest that firms experience significant financial losses as a result of information security breaches (Johnson & Pyke, 2000). We find a highly significant negative market reaction to information security breaches involving unauthorized access to confidential data (Campbell et al., 2003). There is also a substantial amount of anecdotal evidence and self-reported survey data that suggests substantial economic costs are associated with information security

breaches. For example, on February 10, 2000, *The Wall Street Journal* reported that a denial-of-service attack against Yahoo!, "brought Yahoo!'s Web site to its knees, costing it an estimated $ 500 000 in a scant three hours" (Campbell et al., 2003; Johnson & Pyke, 2000) As reported in *CIO*, The Yankee Group estimated the total losses related to the February 2000 denial of service attacks were $ 1.2 billion (Genusa, 2001). A report by (Snider, 2013; Ziobro, 2014) also indicates that the earnings of Target's firm dropped by 46% due to an information security breach that hit the firm in 2013.

It is also found out that breached firms regularly find that potential customers choose to buy from their rivals after finding out that their personal information has been compromised (Kerschbaum et al., 2001). As a result, empirical research finds that firms experiencing security breaches suffer a decrease in stock price on average in the short-term (Benesh, and Clark, 1994; Geczy, 2000; Myers & Ridge, 2008) and long-term (Campbell et al., 2003; Warner, 1980). It is again noteworthy that information security breaches impose organizational costs because firms expend considerable efforts to understand the nature of the breach and mend their security protocols to prevent the breach from recurring (Benesh & Clark, 1994). A few studies have observed a drop in market valuation over one or two days due to security incidents. (Campbell et al., 2003; Cavusoglu et al., 2014). Even though the effects of this information security breach are short-lived, it cannot be glossed over because if one subscribes to the theory of the rational market, he/she will appreciate the fact that these market devaluations should indicate significant financial reversals (Kannan et al., 2007). It was reported by the United Nations in 2005 that several tens of dollars of worldwide economic damage are attributed to compromises in information security (UN 2005, p. xxiii). Breach of an organization's information security system is a matter of concern given the fact that

close to 3 percent of the organization's annual profits are lost due to employees' behavior that results in information security breaches (McIlwraith, 2016). As asserted by (Kedrosky, 2000; Skotnes, 2015).

There is a negative market reaction anytime it is detected that there has been a breach in the information resources especially when the breach involves illegal access to customers' confidential information (Campbell et al., 2003). Even though an argument exists that seeks to discredit the economic impact of information security breaches on firms, it should be noted that there is always a long-term effect of breaches on the affected firms. This is because, any time a breach occurs, firms spend money to take the necessary actions to prevent future occurrences (Bridis, 2001).

When the breach involves leakage of customers' confidential information or theft of proprietary information, the economic effect on the organization is very high (Campbell et al., 2003; Power, 2002). Information security breaches can also create a greater sense of insecurity among customers which can lead to loss of trust and confidence (Cavusoglu et al., 2014). The direct monetary loss involved in such situations is long-term but very consequential on the breached firm. The cost/loss associated with information security breaches of organizations could be short-term, that is, within the space of time during which the breach occurred or it can span over some time (long-term) (Cavusoglu et al., 2014). In the short term, the costs are normal results of inaccessibility of critical information resources and lack of resources to immediately resolve the breaches (D'Amico, 2000). Long-term costs include loss of trust and confidence in the organization especially when the breach involves leakage of or loss of integrity of customers' confidential information, customers switching to competitors,

and battling of legal issues as a result of the breach. It should be added that as time passes by, breached firms experience a decline in returns (Bharadwaj et al., 2009) and the response/attitude of customers is likely to change from positive to negative (Subramani, & Walden, 2000). These notwithstanding, the type of a particular cost associated with a breach is not always identifiable since different firms adopt different strategies to handle information security breaches (Cavusoglu et al., 2014).

The incidence of information security breaches puts the credibility of the breached firm at a very low profile which prevents investors from doing business with that firm (Fama et al., 1969). This weakens the competitive strength of the breached firm. Internet-only buying and selling firms stand the risk of losing business when there is a recurring incidence of the information security breach as it is already evident that most people dislike any form of online business for fear of theft involving credit card information (Angus Reid, 2000).

It is shown that the information security breach that occurred between 1996 and 2002 brought a deleterious effect on the returns of the breached firms (Garg, A., Curtis, J. and Halper, 2003), and the effect, in terms of assets and capital was greater for online firms (Cavusoglu, Mishra, and Raghunathan, 2004). There are also long-term adverse effects on the stock price of breached companies especially when it becomes apparent that the breach resulted from the company's inability to safeguard customers' confidential information (Yayla & Hu, 2011). One of the big financial blows to breached firms is that their customers turn to their (breached firms) competitors for the services they need (Gupta, 2012). This results in both long-term and short-term decreases in their stock prices (Campbell et al., 2003; Kannan et al., 2007; Malhotra, 2010).

In conclusion, there is no doubt that the financial cost that comes with information security breaches has significant effects on organizations (Campbell et al., 2003) and the cost could be both tangible and intangible (D'Amico, 2000). There is a substantial fall in the market value of companies that experience information security breaches (Bharadwaj et al., 2009), and the loss of the market value is estimated at 2.1%. When this is quantified in monetary terms, it stands at the average cost of $1.65 billion. (Cavusoglu et al., 2014).

Empirical evidence from the study conducted by (Cavusoglu et al., 2014) shows that

a. "Breach cost is higher for "pure-play," or Internet-only, firms than for conventional firms."
b. "Breach cost increased during the study period."
c. "Security breaches are costlier for smaller firms than larger firms."
d. "Breach cost is not significantly different across breach types."

This then shows that for every breach in the information resources of a firm, there is an associated loss which is relatively consequential and detrimental to the breached firm (Deane et al., 2019).

***Hypotheses 3**: Information security breaches have serious consequences on organizations' economic position*

CHAPTER THREE

METHODOLOGY

3.1 Introduction

Research methodology is a systematic approach to issue solving. It can be defined as a science that investigates how research should be conducted. It describes the step-by-step activities that researchers use to get their work done, as well as the research process itself. It is also used to describe, explain, and predict for diverse phenomena (Myers, 2010). It serves as a road map to researchers (Desai, 2020). This section deals with the research design process, the systematic approach to the data collection, data analysis, and validation. The researcher also discusses the ethical considerations in conducting the study.

3.2 Research Design Process

A quantitative survey method was adopted to explore the various hypotheses outlined in this study. The relationship among the various constructs of the study was also tested based on rigorous statistical analysis. To gather the information needed to investigate the hypotheses, a thorough questionnaire was used. The instruments were developed from existing studies by researchers (Ali et al., 2020), 2020; Bulgurcu et al., 2010; Chen et al., 2016; Herath & Rao, 2009; Sohrabi Safa et al., 2016, Cardinal, 2015; Colton & Kirsch, 1996, 1996; Eisenhardt, 2008) and modified to suit this study. The questionnaire was structured as follows:

3.2.1. Information Security Policy Compliance

Respondents were asked to give an account of the perceived benefits that their organizations enjoy as a result of employees' compliance with the Information Security Policy. The degree of importance is measured using a five-point Likert scale (1= Strongly Agree to 5 = Strongly Disagree).

3.2.2. Factors that Influence Information Security Policy Compliance

This section was meant to explore whether employees' attitude and behavior can influence their compliance with the information security policies of the organization. Again, it sought to investigate the effects of reward and punishment on information security policy compliance. The section also collected data to find out what drives employees to develop good intentions towards ISP compliance. Five-point Likert scale was used to evaluate respondents' level of agreement or disagreement (i.e., 1 = Strongly Agree and 5 = Strongly Disagree).

3.2.3. Information Security Breaches on Revenue

Respondents were asked to describe the frequency and severity of security breaches on the organization's revenue base. The severity of the breaches was evaluated using a five-point Likert scale ("1=Strongly Agree" to "5= Strongly Disagree"). In addition to the above, the respondents were asked to report on the control variables such as the availability of information security policies in the organization, efforts by management to ensure compliance, other factors that increase the organization's revenue, and security culture. Security culture was included because two different organizations were considered for the study and the respondents were required to briefly describe the security culture that pertains to their organization (Banerjee, Cronan & Jones, 1998; D'Arcy et al., 2009; Siponen et al., 2000).

3.3 Population and Sampling Procedure

The population considered for this was employees from four different companies all located in Kumasi in the Ashanti region of Ghana. Two of the companies (one public and one private) are into the production and distribution of drinks. One of the companies also deals in different kinds of ventures including production and distribution of drinks, multimedia broadcasting, production and distribution of herbal drugs, and school. The other company also manufactures and distributes roofing sheets. All these companies consider information as the key resources of the organization. The companies' websites and other online platforms are the major platforms for the marketing of their products. The companies sell to their customers in wholesale.

The information they keep about their organizations and the customers are very critical to them because the customers (who are mainly with the consumers) easily switch patronage with the slightest reduction in sales. The focus was on the employees who were in charge of the company's critical information resources therefore a convenient sampling technique was used (Saunders, Lewis & Thornhill, 2012). The departmental/unit heads assisted the researcher to find these employees and 70 participants were obtained from the four companies.

3.4 Data Collection

A pre-test was conducted to test the applicability and understandability of the research instrument. The heads of departments and units were chosen for the pre-test. They were chosen because they form part of the management team who are entrusted with the responsibility of making sure all policies in the organization are duly adhered to. The heads were from the Finance, IT/MIS, and Production departments. Ten participants

were chosen for the pre-test. Online self-administered questionnaires were designed using Google Forms for the data collection. Using the online survey was not a problem because the participants were those that mostly use information technology resources and the internet for their daily task. The questionnaire contained 49 items on the main constructs of the study. The reliability of instruments was determined by finding the Cronbach's Alpha of the pre-test questionnaire using IBM SPSS v26. The results revealed some inconsistencies in the test instruments. The test items were then modified to get 57 questions. The questions were readministered after a thorough explanation to the respondents. The questionnaire was then administered on the 70 sampled participants. The questionnaire was thoroughly explained to them after they had all agreed to take part in the survey. A Google Form link containing the questions was sent to them on their WhatsApp lines through their Departmental heads. The participants were entreated to complete and return the survey instruments within two weeks.

3.5 Data Analysis Technique

A quantitative descriptive design was used to collect information from the students on the constructs of the study. The researcher deemed it necessary to define the confines of these variables with the expectation to draw statistical conclusions based on sets of assumptions (Sandelowski, 2000). This method is also seen as appropriate when participants' perceptions about the importance of a current phenomenon are examined (Lodico, Spaulding, & Voegtle, Lodico, Spaulding & Voegtle, 2010). Specific questions were asked to collect data from the participants and the data were objectively analyzed using statistics. The reliabilities of the various constructs were tested using Cronbach's alpha and the values obtained suggest that the instruments developed were reliable and valid (Brownlow, 2004). The values are shown in Table 3.1.

3.6 Validity and Reliability

The reliability of instruments was determined by finding the Cronbach's Alpha of the items on the questionnaire using IBM SPSS v26. The results indicated a high reliability of the test items because their values exceeded the recommended threshold of >.70 (Nunnally, 1978). This is shown in Table 3.1.

Table 3.1: Reliability Statistics of Constructs

Scale	Cronbach's Alpha	No. of Items
Perceived Significance of ISP Compliance	.880	11
Factors that Influence Employees' compliance	.869	29
Effects of Information Security Breaches on Revenue	.757	16

3.7 Ethical Consideration

Articles, journals, and conference papers cited in this study are properly cited. The responses of the participants will be kept strictly confidential. The findings of the study will not be used publicly or privately to malign the participating organizations.

CHAPTER FOUR

PRESENTATION OF RESULTS AND DISCUSSION

4.1 Introduction

This section presents the results of the participants' responses. Agree and Strongly Agree were combined to represent respondents' agreement with the question answered. Also, Disagree and Strongly Disagree were combined to represent the respondents' disagreement with the question asked. Neutral response means that the respondents could not give definite answers to the questions asked. They were not sure of the answers or not aware of the incidence being referred to. Therefore, attention is given to those questions which respondents indicated their agreement or disagreement unless those in the neutral bracket are in the majority.

4.2 Presentation of Results

4.2.1 Demographies

The demographic characteristics of the participants are summarized in the Tables 4.1, 4.2, 4.3, 4.4, and 4.5.

Table 4.1: Respondents' Gender

Gender	Frequency	Percent (%)
Female	7	10
Male	63	90
Total	**70**	**100**

Table 4.1 indicates that 7 (10%) of the respondents were female while 63 (90%) were males.

Table 4.2: Respondents' Age Distribution

Age	Frequency	Percent (%)
18-23	7	10
24-28	14	20
29-34	14	20
41-46	21	30
47-52	7	10
53-58	7	10
Total	**70**	**100**

Table 4.2 indicates that 7 (10%) of the respondents were between the ages of 18 and 23 years, 14 of them (20%) were between 24 and 28 years, 14 of them (i.e., 20%) were between 29 and 34 years, 21 of them (30%) were between the ages of 41 and 46 years, 7 (10%) of them were between the ages of 47 and 52 years while 7 (10%) of them were between the ages of 53 and 57 years. It is seen from the results that the majority of the respondents (80%) were young (i.e., 18 – 46 years). Therefore, they are likely to find it easy to understand computerized information systems.

Table 4.3: Respondents' Company

Company Type	Frequency	Percent (%)
Private	63	90
Public	7	10
Total	**70**	**100**

Table 4.3 indicates that 63 of the respondents, representing 90% were from the three private companies while 7 (10%) were from one public company.

Table 4.4: Respondents' Department

Department	Frequency	Percent (%)
Accounts	7	10
IT/MIS	7	10
Production	56	80
Total	**70**	**100**

From Table 4.4, majority of the respondents (80%) were from the production department, 7 of the respondents (10%) were from the Accounts department while 7 of them (10%) were also from the IT/MIS department.

Table 4.5: Respondents' Work Experience

Work experience	Frequency	Percent (%)
2-7 years	49	70
8 - 13 years	14	20
Less than 2 years	7	10
Total	**70**	**100**

The majority of the respondents (70%) have spent between 2 and 7 years in their company, 14 of them (20%) have also spent between 8 and 13 years whiles only 7 (10%) have spent less than 2 years in their company

4.2.2 Q1: What are the workers' perceptions about the need for compliance with information security policy in organizations?

The majority of the respondents (90%) indicated that compliance with the ISP enhances their performance while 70% further indicated that the entire security of the information resources of their companies depends on employees complying with the ISP requirements. 90% of them also said that compliance with ISP has a positive impact on

the overall performance of the organization and further indicated that non-compliance puts the organization's assets and business in danger. However, 50% of them said their organizations have not experienced any setback due to a lack of compliance from employees. Also, almost all the respondents (90%) agreed that the best way to mitigate the risk of information security breaches in an organization is through compliance with the security requirements. All the respondents indicated that when their organizations have a competitive advantage due to their compliance with the information security requirements of their organization. It was further revealed by 80% of the respondents that the confidentiality and integrity of the information resources of the organizations are guaranteed as a result of ISP compliance.

Moreover, 42 respondents (60%) indicated that compliance with information security policies has a direct impact on the organization's revenue. However, only 40% of the respondents indicated that their managers are mostly in dilemma due to non-compliance with information security policies. The results are summarized in Table 4.6.

Table 4.6: Customers' perceived importance of ISP compliance

Items	Agree		Neutral		Disagree	
	Frequency	(%)	Frequency	(%)	Frequency	(%)
Compliance with information security requirements enhances my performance.	63	**90**	7	**10**		**0**
The security of the company's information resources entirely depends on the employee's compliance.	49	**70**	7	**10**	14	**20**
Noncompliance puts the organization's assets and business in danger.	56	**80**	7	**10**	7	**10**
Compliance with information security policy can mitigate the risk of information security breaches in the organization	63	**90**	0	**0**	7	**10**
Information security policy compliance has a positive impact on the overall performance of the organization	63	**90**	0	**0**	7	**10**
The organization has experienced setbacks before due to a lack of compliance from the employees	7	**10**	28	**40**	35	**50**
Compliance with the information security policy gives the organization a competitive advantage	100	**100**	0	**0**	0	**0**
Compliance with the organization's information security policy has a direct effect on the organization's income	42	**60**	21	**30**	7	**10**
The confidentiality and integrity of the company's information resources are guaranteed because employees comply with the information policies.	56	**80**	14	**20**	0	**0**
Management of the organization is in a dilemma most of the time due to noncompliance with the information security policies	49	**70**	21	**30**	0	**0**
Customers have expressed goodwill in the organization due to our information security policy structures	42	**60**	28	**40**	0	**0**

4.2.1 Q2: What are the factors that motivate employees of an organization to comply with information security policies?

Almost all the respondents (90%) agreed that their organizations have adopted strategies that influence their employees to comply with the information while 70% of them indicated that reward is not part of these strategies. The majority of the respondents, 50% in all indicated that rewards, in the form of material, appreciation, acknowledgment by superiors, and appreciation are not part of the strategies employed to motivate compliance of ISP. An average of 21 respondents said these forms of reward are applied in their organizations. But 90% of the respondents' said punishment is part of the strategies that are employed by management to ensure compliance with the organization's ISP whiles 80% indicated the punishment is well enforced. The punishment takes the form of reprimand (whether written or oral) as indicated by 80% of the respondents. Monetary or non-monetary penalties are forms of punishment against employees who do not comply with ISPs. This was indicated by 50% of the respondents and only 30% of them disagreed with it.

The majority of the respondents (80%) said that they are disciplined when they break information security rules and further indicated that those who repeatedly breach security rules risk the termination of their appointment. Only 21 of the respondents said that the nature of their work is such that they have no other option than to ensure confidentiality and privacy of the organization's information resources. It means that the majority of the respondents choose to comply with their organization's ISP. The majority (80%) of the respondents said that they feel morally obliged to comply with their organization's ISP and the same percentage of the respondents indicated that they feel so guilty if they don't comply with their organization's ISP. 60% of the respondents

also indicated that they comply with their organization's ISP not because it is favorable to them while 80% claimed they also comply with their organization's ISP requirements not because the requirements are realistic and flexible. Eight (80%) of them also said they comply with their organization's ISP requirements because that enhances their performance and also helps the organization to achieve its goals. Seven, representing 70% indicated that their organizations' ISP requirements address their concerns with regards to their organizations' ISP while all of them claimed that compliance with their organizations' ISP rules protects their organizations' Information systems. Respondents were asked if they would not comply with ISP requirements because of the following: the requirements are not favorable to them, they are unrealistic and rigid, they delayed their performance, or hold them back from performing their actual work. To any of these statements, almost all the respondents (90%) disagreed.

Even though the majority of the respondents said that rewards are not part of the strategies employed by their managers to motivate them to comply with their organizations' ISP, they all indicated that if rewards are employed, they will have a very high influence on the employees' compliance with the organizations' ISP. However, the respondents were split over the influence of punishment on employees' compliance with their organizations' ISP even though studies affirm that it has a deterrent force that can result in positive outcomes.

The results are summarized in Table 4.7.

Table 4.7: Factors that Motivate Employees' Compliance

Items	Agree		Neutral		Disagree	
	Frequency	(%)	Frequency	(%)	Frequency	(%)
The organization has adopted strategies that influence employees to comply with the information security requirements	63	**90**	0	**0**	7	**10**
A reward is one of the main strategies employed by my organization to ensure compliance with information security policies	7	**10**	14	**20**	49	**70**
The Reward for Information Security Policy (ISP) Compliance is very well enforced	14	**20**	7	**10**	49	**70**
Punishment is one of the main strategies employed by the organization to ensure compliance with information security policies	63	**90**	0	**0**	7	**10**
The punishment for noncompliance to Information Security Policy (ISP) is very well enforced	56	**80**	0	**0**	14	**20**
If I comply with information security policies, I will get a material reward	7	**10**	7	**10**	56	**80**
If I comply with information security policies, I will get appreciation	28	**40**	7	**10**	35	**50**
If I comply with information security policies, I will get acknowledgment from my superior	21	**30**	14	**20**	35	**50**
If I comply with information security policies, I will get a promotion	28	**40**	7	**10**	35	**50**
If I do not comply with information security policies, I will get punished or demoted	63	**90**	0	**0**	7	**10**
If I do not comply with information security policies, I will receive a personal reprimand in oral or written assessment reports	56	**80**	0	**0**	14	**20**
If I do not comply with information security policies, I incur monetary or non-monetary penalties	35	**50**	14	**20**	21	**30**
The organization disciplines employees who break information security rules	56	**80**	7	**10**	7	**10**
The organization terminates the appointment of the employees who repeatedly break security rules	56	**80**	7	**10**	7	**10**
The information I deal with in my daily work is such that it is imperative to ensure confidentiality and maintain privacy.	21	**30**	14	**20**	35	**50**

I feel morally obligated to comply with the organization's ISP	56	**80**	7	**10**	7	**10**
I feel guilty if I do not comply with the organization's ISP	56	**80**	7	**10**	7	**10**
It is favorable to me	28	**40**	28	**40**	14	**20**
It is realistic and makes work flexible	56	**80**	0	**0**	14	**20**
It helps to achieve the organization's goals	56	**80**	0	**0**	14	**20**
It enhances my performance	56	**80**	7	**10**	7	**10**
It addresses my concerns in respect of the existing ISP	49	**70**	14	**20**	7	**10**
It protects the organization's information systems	70	**100**	0	**0**	0	**0**
It is not favorable to me	0	**0**	7	**10**	63	**90**
It is unrealistic and rigid	0	**0**	7	**10**	63	**90**
It delays work/stills performance	0	**0**	7	**10**	63	**90**
It holds me back from doing my actual work	0	**0**	7	**10**	63	**90**
	High		**Neutral**		**Low**	
	Frequency (%)		**Frequency (%)**		**Frequency (%)**	
If the organization adopts reward strategies to ensure compliance, what is the degree of its influence on the employees' compliance with the information security measures?	42	**60**	0	**0**	28	**40**
If the organization adopts punishment strategies to ensure compliance, what is the degree of its influence on the employees' compliance with the information security measures?	35	**50**	0	**0**	35	**50**

4.2.3 Q3: To what extent do information security breaches affect an organization's revenue?

Five of the respondents, representing 50% said that their organizations have never experienced incidents of information security breaches while only 14 (20%) indicated that their organization has experienced information security breaches before. The others said they have no idea about that. However, 70% of them indicated that frequent occurrence of information security breaches can have a severe impact on their organizations' income. 41.5% of the respondents said that their companies have lost some customers due to information security breaches while 30% said such incidence has never occurred in their organization.

However, 28.5% of them said they have no idea about such incidence in their organizations. Moreover, 42.9% of the respondents indicated that some investors stopped working with them due to information security breaches while 30% said they have never experienced such situations in their company. With regards to post-attack remedies, majority of the respondents, an average of 60% said that their organizations have not spent any huge sum of money to curb the situation while an average of 10% indicated that relatively huge sum of money has been spent on that. The post-attack remedies include but not limited to replacing computer software, hiring an expert to manage breached information resources and compensating customers who are victims of the information breaches. 29 respondents (41.5%) said that their organization has lost some customers due to information security breaches while 21 (30%) said they have not lost any customers due to any breaches. 30% remained neutral to the question. Again, 34 (48.6%) of the respondents said that their organizations have not faced any legal actions from any customer or entity due to information security breaches. 40% of

them also claimed they do not know whiles only 8 agreed that their organizations have faced legal actions due to IS breaches. Also, 60% of the respondents disagree that breaches in the information resources of an organization are inconsequential to the capital growth of the company. 30% of them remain neutral while only 10% agreed that breaches are inconsequential to the capital growth. Also, 60% of them disagree that the impact of information security breaches on organizations is insignificant; only 30% of them registered their agreement while 10% remained neutral. 56 of the respondents, representing 80% indicated that their organizations will lose customers if secret ingredients are made known to competitors.

Only 10% of them disagreed while 10% remained neutral. 80% of them also indicated that their organization has experienced information security breaches before but it didn't have any direct severe impact on production and sales while 20% disagreed with it. However, 50% of the respondents testified that their organizations experienced financial loss at the end of the accounting year in which breaches occurred while 50% indicated that no loss occurred in that accounting year when the breach occurred. The results are summarized in Table 4.8.

Table 4.8: Effects of ISP Breaches on Organizations' Revenue

Iteams	Agree		Neutral		Disagree	
	Frequency	(%)	Frequency	(%)	Frequency	(%)
The company has recorded an incident of information security breaches.	14	**20**	21	**30**	35	**50**
Frequent occurrence of information security breaches in the organization can severely affect the income of the company?	48	**70**	7	**10**	14	**20**
The company has lost some customers in the past years due to information security breaches.	29	**41.5**	20	**28.6**	21	**30**
The organization has lost some investors due to information security breaches.	30	**42.9**	19	**27.1**	21	**30**
The organization has spent a relatively huge sum of money replacing computer software due to virus attack	7	**10**	19	**27.1**	44	**62.9**
The organization has spent money to hire experts to manage its information resources after security breaches	7	**10**	20	**28.6**	43	**61.8**
The company has spent a huge sum of money on post-attack remedies.	7	**10**	20	**28.6**	43	**61.4**
The organization has faced legal actions before because of breaches in its information security resources	8	**11.4**	28	**40**	34	**48.6**
The organization has paid money to compensate customers due to Information Security breaches	14	**20**	28	**40**	28	**40**
There was a reduction in sales because Customers complained that they were not able to access our website or any of our platforms.	0	**0**	48	**68.6**	22	**31.4**
Breaches in the information resources are inconsequential to the capital growth of the organization.	7	**10**	21	**30**	42	**60**
The impact of the information breaches on the organization is insignificant	21	**30**	7	**10**	42	**60**
The organization will lose its competitive power when Secret ingredients and the process of manufacturing our products are released to outsiders	56	**80**	7	**10**	7	**10**
The organization has experienced information security breaches before but they didn't have any severe direct impact on production and sales	56	**80**	0	**0**	14	**20**
The organization has experienced information security breaches before but its impact on production and sales was not noticed	56	**80**	0	**0**	14	**20**
The organization has experienced information security breaches before and the organization recorded a loss for that accounting year	35	**50**	0	**0**	35	**50**

4.3 Discussion of Results

This section discusses the finding of the study in relation to the research questions.

4.3.1 Perceived importance of Information security policy compliance

The study revealed that information security policy compliance enhances workers performance and also ensures the security of the organization's information resources as postulated by similar studies (Boss et al., 2009; Yazdanmehr et al., 2020). Also, the study confirms that if workers continue to ignore security policies, the organization's assets are put in danger (Hair, Black, Babin, Anderson & Tatham, 2006). Compliance with the Organizations' ISPs has a positive impact on the overall performance of organizations as also postulated by.

Moreover, the study also revealed that compliance with the organizations' ISPs remains the best way to mitigate against the information security breaches in the organizations. This is also consistence with the findings of similar studies (Cheng et al., 2013; Ifinedo, 2014; Pahnila et al., 2007; Siponen et al., 2014). Also, it is affirmed by the study that organizations that practice compliance have a highly competitive advantage (Deane et al., 2019; Desai, 2020). It is also revealed that customers have confidence in organizations that adhere to information policy requirements. All these notwithstanding, and contrary to findings, it is indicated that managers are not mostly in dilemma due to non-compliance with information security policies. Given the above findings, Hypothesis 1: Information security policy compliance is very necessary for the security of the information resources of every organization, is validated.

4.3.2 Factors that motivate employees to comply with Information Security Policies

Even though the majority of the respondents said that rewards are not part of the strategies employed by their managers to motivate them to comply with their organizations' ISP, they all indicated that if rewards are employed, they will have a very high influence on the employees' compliance with the organizations' ISP. Therefore, the study confirms that rewards have a positive influence on security policies' compliance (D'Arcy et al., 2009; Zenger, 1992) However, as in the case of several studies, the respondents were split over the influence of punishment on employees' compliance with their organizations' ISP (Boss et al., 2009; Chen et al., 2015; Eisenhardt, 2008).

The study also revealed that most employees comply with organizations' ISPs because they feel morally obliged to do so. These moral obligations are the self-imposed prohibitions adopted by employees to achieve expected outcomes. Self-guilt is also one of the factors that motivate employees to comply with the organizations' ISPs. Moreover, as revealed by several study outcomes, it is confirmed that employees also comply with information security policies when they know that it improves their performance. Also, employees comply with information security policies when they perceived that compliance helps the organization achieve its goals and protect its information resources (Al-omari & El-gayar, 2012). Therefore, Hypotheses 2A: Factors that influence employees to comply with information security policies are mostly those that deal with employees' behavior/attitude and application of a stimulus, is sustained.

Also, Hypothesis 2B: Employees develop good intention to comply with information security policies when they perceive that the policies suit/benefit them and also contribute to something worthwhile, is validated

4.3.3 Effects of Security Breaches on Revenue

It was admitted that the frequent occurrence of information security breaches has an impact on the organizations' revenue. However, they further indicated that such impact is not noticed. This is probably because the cost associated with security breaches are not always identifiable as indicated by (Cavusoglu et al., 2014). Also, this explains why the majority of the respondents indicated their organizations have experienced information security breaches before but they didn't have any direct severe impact on the organizations.

Even though the employees were not able to identify the direct consequences of ISP breaches on the organizations' revenue, as in the case of several findings from similar studies (Bharadwaj et al., 2009; Cavusoglu et al., 2014; D'Amico, 2000), they disagreed that the impact of security breaches on organizations' capital growth is inconsequential or insignificance. The results also indicated that it is not certain that organizations lose customers or investors when information security breaches occur. The study thus shows that in as much as information security policy compliance is very beneficial for organizational growth, it is quite difficult to quantify its direct impact on the organizations' capital growth. Thus, Hypotheses 3: Information security breaches have serious consequences on organizations' economic position, cannot be validated because the employees were not certain about the direct consequences of information security breaches on the organization's revenue.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusion

The study aimed at finding out the extent to which compliance with the information security policies influences organizations' capital growth. To achieve this, three variables were exploited. First, the perceived significance of information security policy compliance. It study revealed that employees believe that compliance with information security policies remains the best way to ensure the confidentiality, integrity, and availability of information resources of an organization. secondly, factors that motivate employees to comply with information security policies. The study revealed that none of the participating companies employs rewards to ensure compliance however, the employees said rewards could have been the best option to ensure compliance instead of the punishment. Also, the employees confirmed that the outcome of compliance serves as the major factor that motivates them. Thirdly, the effects of security breaches on revenue. The employees admitted that the effects of information security breaches on the organization's revenue cannot be directly measured especially in monitary terms but they believe that the effects are consequential.

5.2 Recommendations

Even though the findings of this study are not far different from many research findings, it is still recommended that a more pragmatic approach is used to investigate the phenomenon in different companies. This is because the study employed a quantitative approach in manufacturing companies that rarely keep customers' confidential data. A qualitative approach can be used to examine the phenomenon in a financial organization that deals with customers' and employees' sensitive information.

The study also recommends that just as punishment is highly enforced to ensure compliance, rewards must equally be applied to motivate employees to comply with security policies.

REFERENCES

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, *32*(4), 665–683. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x.

Ajzen, I., & Fishbein, M. (1975). A Bayesian analysis of attribution processes. *Psychological Bulletin*, *82*(2), 261–277. https://doi.org/10.1037/h0076477

Akturk, A. O., Izci, K., Caliskan, G., & Sahin, I. (2015). *Analyzing Preservice Teachers Attitudes towards Technology*. *9*(12), 3960–3966.

Al-omari, A., & El-gayar, O. (2012). *Security Policy Compliance : User Acceptance Perspective*. 3317–3326. https://doi.org/10.1109/HICSS.2012.516.

Albrechtsen, E. (2007). *A qualitative study of users' view on information security. Computers & Security 26(4),*. 276–289.

Ali, R. F., Dominic, P. D. D., & Ali, K. (2020). Organizational governance, social bonds and information security policy compliance: a perspective towards oil and gas employees. *Sustainability (Switzerland)*, *12*(20), 1–27. http s://doi.org/10.339 0/su12208576.

Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. *Information and Computer Security*, *26*(4), 420–436. https://doi.org/10.1108/ICS-09-2017-0063.

Anders, G. (2000). *eBay's CEO reacts to hacker attack, seeks joint action on Web security. Wall Street Journal*. *B18.*

Andreoni, J., Harbaugh, W., & Vesterlund, L. (2003). The carrot or the stick: Rewards, punishments, and cooperation. *American Economic Review*, *93*(3), 893–902. https://doi.org/10.1257/000282803322157142.

Angus Reid, G. (2000). *Security and Privacy Issues Keeping Millions from Shopping Online. Angus Reid Group, April 27, 2000 (www.ipsos-na.com/ news/pdf/media/ap000426.pdf).*

Anthony, J.H., Choi W., & S. G. (2006). *Market reaction to e-commerce impairments evidenced by website outages, International Journal of Accounting Information Systems 7,* 60–78.

Axelrod, LJ and Newton, J. (1991). *Preventing nuclear war: beliefs and attitudes as predictors of disarmist and deterrentist behavior. Journal of Applied Social Psychology 21*(1),29–40.

Banerjee, D.; Cronan, T.P.; & Jones, T. W. (1998). *Modeling IT ethics: A study of situational ethics. MIS Quarterly, 22*(1). 31–60.

Barnard, L., Solms, R. Von, Studies, C., Technikon, P. E., Elizabeth, P., Studies, C., Technikon, P. E., & Elizabeth, P. (1999). *The evaluation and certification of information security against BS 7799*.

Baxter, P., & Jack, S. (2008). *Qualitative case study methodology: Study design and implementation for novice researchers. The qualitative report, 13*(4): 544-559.

Beautement, A., Sasse, M. A., & Wonham, M. (2008). *The Compliance Budget : Managing Security Behaviour in Organisations*.

Bedford, M. (2008). *The 2008 insider threat survey: Workers admit to everyday behavior that puts sensitive business information at risk. White paper, RSA, Bedford, MA, The 2008 insider threat survey: Workers admit to everyday behavior that puts sensitive business information*.

Benesh, G.A., & Clark, J. A. (1994). *The value of indirect investment advice: stock recommendations in Barron's, Journal of Financial and Strategic Decisions*. *7*, 35–43.

Bharadwaj, A., Keil, M., & Mähring, M. (2009). Effects of information technology failures on the market value of firms. *Journal of Strategic Information Systems*, *18*(2), 66–79. https://doi.org/10.1016/j.jsis.2009.04.001.

Bloom, M. C., & Milkovich, G. T. (2017). *Working Paper Series The Relationship Between Risk , Incentive Pay , and Organizational Performance*.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151–164. https://doi.org/10.1057/ejis.2009.8.

Bridis, T. (2001). *E-Business: Microsoft takes steps to thwart hacker attacks, The Wall Street Journal*.

Brownlow (2004). *SPSS explained*. London: Routledge.

Buckman, T. B. & R. (2001). *Microsoft lays 2nd-day woes on hackers, The Wall Street Journal*.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly: Management Information Systems*, *34*(SPEC. ISSUE 3), 523–548. https://doi.org/10.2307/25750690.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empi...: EBSCOhost. *Journal of Computer Security*, *11*(11), 431–448. http://cit eseerx.ist.psu.edu / viewdoc/download?doi=10.1.1.83.7735&rep=rep1&type=pdf%0Ahttps://web-a-ebscohost-com.libproxy.smu.edu.sg/ehost/pdfviewer/pdfviewer?vid=1&sid=e13ea18f-2e81-45a7-b39f-3dea6201f87c%40sdc-v-sessmgr06

Cardinal, L. B. (2015). *Technological Innovation in the Pharmaceutical Industry : The Use of Organizational Control in Managing Research and Development Technological innovation in the pharmaceutical industry: The use of organizat ... September*. https://doi.org/10.1287/orsc.12.1.19.10119.

Cavusoglu, H., Mishra, B. & Raghunathan, S. (2004). *The Effect of Internet Security Breach Announcements on the Market Value: Capital market reactions for breached firms and Internet security developers, International Journal of Electronic Commerce*. *9*(1), 69–104.

Cavusoglu, H., Mishra, B. & Raghunathan, S. (2005). *The Value of Intrusion Detection Systems in Information Technology Security Architecture, Information Systems Research 16*(1): 28–46.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2014). *The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers The Effect of Internet Security Breach Announcements on Market Value: 4415*(October 2015). https://doi.org/10.1080/10864415.2004.11044320.

Chen, Y., Ramamurthy, K. R., Wen, K., Ramamurthy, K. R. A. M., & Wen, K. (2016). *Impacts of Comprehensive Information Security Programs on Information Security Culture Programs on Information Security Culture*. *4417*(February). https://doi.org/10.1080/08874417.2015.11645767.

Chen, Y., Ramamurthy, K., & Wen, K. (2015). *Journal of Management Information Organizations ' Information Security Policy Compliance : Stick or Carrot Approach ?* 37–41. https://doi.org/10.2753/MIS0742-1222290305.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers and Security*, *39*(PART B), 447–459. https://doi.org/10.1016/j.cose.2013.09.009

Coates H, James R, Baldwin G (2005). A critical examination of the effects of learning management systems on university teaching and learning. *Tertiary Educ. Manage. 11:19-36.*

Colton, D., & Kirsch, A. (1996). *My IOPscience A simple method for solving inverse scattering problems in the resonance region*. *383*.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security*, *32*, 90–101.https://doi.org/10.1016/j.cose.2012.09.01

CSC (2019). *CSC survey reveals inadequate information security practices among companies worldwide. Available at www.csc.com/ newsande vents/ne ws/1584 .shtml.*

D'Amico, A. D. (2000). *What does a computer security breach really cost. Secure Decisions, Applied Visions Inc.*

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. https:// doi.org/10.128 7/isre.1070.0160.

Da Veiga, A. & Eloff, J. H. P. (2010). *A framework and assessment instrument for information security culture. Computers & Security, 29(2): http:// linki nghu b .esevier.com/retrieve/pii/S0167404809000923. [March 26, 2014]*. 196–207.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, *35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982.

Deane, J. K., Goldberg, D. M., Rakes, T. R., & Rees, L. P. (2019). The effect of information security certification announcements on the market value of the firm. *Information Technology and Management*, *0123456789*. https ://doi.org /10.1007/s10799-018-00297-3.

Desai, M. R. (2020). *An integrated approach for information security compliance in a financial services organisation*, 274–282.

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers and Security*, *20*(2), 165–172. https://doi.org/10.1016/S0167-4048(01)00209-7.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal*, *19*(4), 391–412. https://doi.org/10.1111/j.1365-2575.20 07.00 289.x

Eisenhardt, K. M. (2008). *Control: Organizational And Economic Approaches *. 31*(2), 134–149.

Ettredge, M.L., & V. J. R. (2003). *Information transfer among Internet firms: the case of hacker attacks*, *Journal of Information Systems*. *17*, 71–82.

Fama, E. F., Fisher, L., Jensen, M. C., & Roll, R. (1969). The Adjustment of Stock Prices to New Information. *International Economic Review*, *10*(1), 1. https://doi.org/10.2307/2525569.

Fulford, H., & Doherty, N. F. (2003). *The application of information security policies in large UK-based organizations: an exploratory investigation*. 106–114. https://doi.org/10.1108/09685220310480381.

Garg, A., Curtis, J. & Halper, H. (2003). *Quantifying the Financial Impact of IT Security Breaches, Information Management & Computer Security*. *11*(2/3), 74–83.

Geczy, C. C. (2000). *Is the Abnormal Return Following Equity Issuances Anomalous ? Is the Abnormal Return Following Equity Issuances Anomalous ? 56*, 209–249.

Genusa, A. (2001). *Conspiracy of silence, CIO 14*(10), 92–96.

Gladwell, M. (2013). *David and Goliath: Underdogs, Misfits, and the Art of Battling Giants. New York: Little, Brown.*

Goel, S., & Crain, J. (2010). *ASIA10Proceedings.pdf*. http://w ww.alb any.edu/iasymp osium/proceedings/2010/ASIA10Proceedings.pdf#page=11.

Gordon, L.A, Loeb, M.P., Lucyshyn, W. & Richardson, R. (2004). *CSI/ FBI Computer Crime and Security Survey, Computer Security Institute, San Francisco, CA.*

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, *19*(1), 33–56. https://doi.org/10.3233/JCS-2009-0398.

Hair, J.F.J., Black, W.C, Babin, B.J, Anderson, R.E., & Tatham, R. L. (2006). *Multivariate data analysis. Sixth ed.*

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6.

Hinde, S. (2002). Security surveys spring crop. *Computers and Security*, *21*(4), 310–321. https://doi.org/10.1016/S0167-4048(02)00404-2.

Höne, K., & Eloff, J. H. P. (2002). Information security policy - What do international information security standards say? *Computers and Security*, *21*(5), 402–409. https://doi.org/10.1016/S0167-4048(02)00504-7.

Hsu, J. S., & Lowry, P. B. (2015). *Information Security Policy Effectiveness The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness*, 0–19.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security - a neo-institutional perspective. *Journal of Strategic Information Systems*, *16*(2), 153–172. https://doi.org/10.1016/j.jsis.2007.05.004.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001.

Iheagwara, C., Blyth, A., & Singhal, M. (2004). *Cost effective management frameworks for intrusion*. *12*, 777–798.

Iolations, P. O. V, & Vance, A. (2010). S Pecial I Ssue N Eutralization: N Ew I Nsights Into the P Roblem of E Mployee I Nformation S Ystems S Ecurity. *MIS Quarterly*, *34*(3), 487–502.

Johnson, M. E., & Pyke, D. F. (2000). A framework for teaching supply chain management. *Production and Operations Management*, *9*(1), 2–18. https://doi.org/10.1111/j.1937-5956.2000.tb00319.x.

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study Fear Appeals and Information Security Behaviors: An Empirical Study1. *Source: MIS Quarterly*, *34*(3), 549–566. http://www.jstor.org/stable/25750691%5Cnhttp://about.jstor.org/terms.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154. https://doi.org/10.1016/S0268-4012(02)00105-6.

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce*, *12*(1), 69–91. https://doi.org/10.2753/JEC1086-4415120103.

Kedrosky, P. (2000). *Hackers prey on our insecurities. The Wall Street Journal*. *A18*.

Kerschbaum, F., Spafford, E. H., & Lafayette, W. (2001). *Using internal sensors and embedded detectors for intrusion detection ∗*.

Kraemer, P. Carayon, and J. Clem, ". (2009). *"Human and organizational factors in computer and information security: Pathways to vulnerabilities," Computers & Security*, *, [. 28*, 509–520.

Kranz, J. J., & Haeussinger, F. J. (2014). Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior. *35th International Conference on Information Systems "Building a Better World Through Information Systems", ICIS 2014*, 1–14.

Ligato, L. (2015). *The 9 biggest data breaches of all time. Huffington Post*.

Lodico, M. G., Spaulding, D. T., & Voegtle, K. H.Lodico, M. G., Spaulding, D. T., & Voegtle, K. H. (2010). *Methods in educational research: From theory to practice (2nd ed. Vol. 28). Hoboken, NJ: John Wiley & Sons. 28*.

Malhotra A, M. C. (2010). *Evaluating customer information breaches as service failures: an event study approach. J Serv Res*. 14:44–59.

Malhotra, Y., Galletta, D. F., & Kirsch, L. J. (2008). How endogenous motivations influence user intentions: Beyond the dichotomy of extrinsic and intrinsic user motivations. *Journal of Management Information Systems*, *25*(1), 267–300. https://doi.org/10.2753/MIS0742-1222250110.

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology*, *28*, 417–442. https://doi .org/10.1 146/an nurev.soc.28.110 601.140 752.

Mcconnell, J. J., West, L., & Muscarella, C. J. (1985). *Corporate Capital Expenditure Decisions and the Market Value of the Firm * 1Introduction The theory rate managers decisions and market value are confronted investment of the firm .' However , with the exception there exists relatively little evidence o*. *14*, 399–422.

McIlwraith, A. (2016). *Information security and employee behaviour: how to reduce risk through employee education, training and awareness.*

Meznar, M. B., Nigh, D., & Kwok, C. C. Y. (1994). Effect of Announcements of Withdrawal from South Africa on Stockholder Wealth. *Academy of Management Journal*, *37*(6), 1633–1648. https://doi.org/10.5465/256803

Myers, M. D. (2010). *Qualitative Research in Business and Management.* London: Sage Publications.

Myers, S. C., & Ridge, B. (2008). *CORPORATE*.

Nagin, D. S., & Paternoster, R. (1993). Enduring Individual Differences and Rational Choice Theories of Crime Paternoster theory has developed along two separate theory rejects the as-. *Law & Society Review*, *27*(3), 467–496.

Niccolai, J. (2000). *Analyst Puts Hacker Damage at $1.2 Billion and Rising, IDG News Service*.

Ning, P., Jajodia, S., & Wang, X. S. (2001). *Abstraction-Based Intrusion Detection In Distributed Environments*. *4*(4), 407–452.

Nunnally, J. C. (1978). *Psychometric Theory. New York: McGraw-Hill,*.

Pahnila, S., Siponen, M., Mahmood, A., Box, P. O., Oulun, F.-, Siponen, E. M., & Pahnila, S. (2007). *Employees' Behavior towar ds IS Secur ity Policy Compliance University of Oulu , Department of Information Processing Department of Information and Decision Sciences , University of Texas at El Paso*. 1–10.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003.

Paternoster, R., & Pogarsky, G. (2009). Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices. *Journal of Quantitative Criminology*, *25*(2), 103–127. https://doi.org/10.1007/s10940-009-9065-y.

Power, R. (2002). *CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends. Computer Security Institute. ,. VIII*, 1.

PricewaterhouseCoopers LLP. (2008). *Strategic and Program Evaluation of the Cumulative Environmental Management Association*. *March*, 32.

Privacyrights.org. (2006). *disclosures of U.S. data incidents. Available at http://www.privacyrights.org/ar/chronDataBreaches.htm, accessed 21 January 2007.*

Rhee H.S., C. Kim, & Y. U. Ryu. (2009). *"Self-efficacy in information security: Its influence on end users'' information security practice behavior," Computers & Security." 28,* 816–826.

Sandelowski, M. (2000). *Focus on Research Methods Whatever Happened to Qualitative Description ?* 334–340.

Saunders, M; Lewis, P; Thornhill, A. (2012). *Research Methods for Business Students* (6th ed.).

Sims, H. P. (1980). Further Thoughts on Punishment in Organizations. *Academy of Management Review*, *5*(1), 133–138. https://do i.org/10.5 465/amr.1980.4288 941

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management*, *51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006.

Siponen, P. & M. (2010). *"Improving Employees'' Compliance Through Information Systems Security Training: An Action Research Study," MIS Quarterly." 34*, 757–778.

Skotnes, R. Ø. (2015). Information & Computer Security Article information : *Information & Computer Security*, *23*(3), 302–316.

Snider, M. (2013). *Target data breach spurs lawsuits, investigations. USA Today, New York.*

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006.

Solms, R. Von, Elizabeth, P., Africa, S., Elizabeth, P., & Africa, S. (2011). *Information security governance control through comprehensive policy architectures*, 11–16.

Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J., Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). *Variables influencing information security policy compliance*. https://doi.org/10.1108/IMCS-08-2012-0045.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255–276. https://doi.org/10.1287/isre.1.3.255.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly: Management Information Systems*, *22*(4), 441–464. https://doi.org/10.2307/249551.

Subramani, M. R., & Walden, E. (2000). *The game of the name: A comparison of capital market reactions to DOTCOM vs. traditional name changes. MIS Research Center. Working paper# 00–14. University of Minnesota, Minneapolis, MN. Available online at http://misrc. umn. edu/wp aper/W orking Papers/Dot*.

Trevino, L. K. (1992). The Social Effects of Punishment in Organizations: A Justice Perspective. *Academy of Management Review*, *17*(4), 647–676. https://do i.org/ 10.5465/amr.1992.4279054.

Tyler, T. R., & Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal*, *48*(6), 1143–1158. https://do i.org/10.54 65/AMJ.2005. 19573114.

Volz, D. H. M. (2016). *Concerned by cyber threat. Obama seeks big increase in funding.* Reuters, London.

Vroom, C., & Von Solms, rossouw. (2004). Towards information security behavioural compliance. *Computers and Security*, *23*(3), 191–198. https://do i.org/10.10 16/ jcose.2004.01.012.

Wang C, C. A. (2013). *HTC employees detained amid tradesecret investigation.* Bloomberg, New Yor*k*.

Warkentin, M., Davis, K., & Bekkering, E. (2004). Introducing the Check-Off Password System (COPS): An advancement in user authentication methods and information security. *Journal of Organizational and End User Computing*, *16*(3), 41–58. https://doi.org/10.4018/joeuc.2004070103.

Weill, P. (1992). The relationship between investment in information technology and firm performance: A study of the valve manufacturing sector. *Information Systems Research*, *3*(4), 307–333. https://doi.org/10.1287/isre.3.4.307.

Weitz, E., University, T. A., Vardi, Y., & University, T. A. (2008). *Understanding and managing misbehavior in organizations*.

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, *26*(1), 60–77. https://doi.org/10.1057/jit.2010.4.

Yazdanmehr, A., Wang, J., & Yang, Z. (2020). *Peers matter : The moderating role of social influence on information security policy compliance*. *September 2019*, 1–54. https://doi.org/10.1111/isj.12271.

Zenger, T. R. (1992). Why Do Employers Only Reward Extreme Performance? Examining the Relationships Among Performance, Pay, and Turnover. *Administrative Science Quarterly*, *37*(2), 198. https://doi.org/10.2307/2393221

Ziobro, P. (2014). *Target earnings slide 46% after data breach. Wall Str J*.

APPENDIX 1

QUESTIONNAIRE ITEMS:

Information security policy compliance.

This is a questionnaire on a study being conducted by a student of Akenteng Appiah MENKA

University of Skills Training (AAMUSTED) to examine some issues relating to Information

Security Policy Compliance (ISP) in organizations. The questionnaire is categorized into four (4) parts and you are required to indicate your agreement, disagreement, or knowledge on each of the questions by ticking [√] the appropriate box that corresponds to each question. Please, be well assured that the responses provided are meant for only academic purposes. Thus, your anonymity and confidentiality (including that of your organization) are assured.

PART 1

This part deals with the respondents' demographics and some general information about the organization's information security culture.

1. Gender: Male [ ] Female [ ]
2. Age: below 18 [ ] 18-23 [ ] 24-28 [ ] 29-34 [ ] 35-40 [ ] 41-46 [ ] 47-52 [ ] 53-58 [ ] 59-64 [ ]
3. Type of company: Public [ ] Private [ ]
4. Department: Human Resource [ ] Accounts [ ] IT/MIS [ ] Marketing [ ] Production [ ] Public Relations [ ] Other (Please Specify)……
   Rank: ……
   Position (if any):……

5. Work experience: Less than 2 years [ ] 2–7 years [ ] 8–13 years [ ] 14-19years [ ] 2025 years 26-31 years [ ]

INFORMATION SECURITY CULTURE OF THE ORGANIZATION

PART 1

EMPLOYEES' PERCEPTION OF THE IMPORTANCE OF ISP COMPLIANCE

This part deals with the employees' perception of the importance of information security policy compliance in the organization. Indicate your agreement, disagreement, or knowledge on each of the questions by ticking [√] the appropriate box that corresponds to each question Please

1= Strongly Disagree 2= Disagree 3= Neutral 4= Agree 5 = Strongly Agree

S/N	**STATEMENT**	**1**	**2**	**3**	**4**	**5**
1	Compliance with information security requirements enhances my performance.					
2	The security of the company's information resources entirely depends on the employee's compliance.					
3	Noncompliance puts the organization's assets and business in danger.					
4	Compliance with information security policy can mitigate the risk of information security breaches in the organization					
5	Information security policy compliance has a positive impact on the overall performance of the organization					

6	The organization has experienced setbacks before due to a lack of compliance from the employees					
7	Compliance with the information security policy gives the organization a competitive advantage					
8	Compliance with the organization's information security policy has a direct effect on the organization's income					
9	The confidentiality and integrity of the company's information resources are guaranteed because employees comply with the information policies.					
10	Management of the organization is in a dilemma most of the time due to non-compliance with the information security policies					
11	Customers have expressed goodwill in the organization due to our information security policy structures					

Part 2

FACTORS THAT MOTIVATE ISP COMPLIANCE

This part also seeks information about the factors that motivate the employees to comply with the information security policies in an organization. Indicate your agreement, disagreement, or knowledge on each of the questions by ticking [√] the appropriate box that corresponds to each question Please

1= Strongly Disagree 2= Disagree 3= Neutral 4= Agree 5 = Strongly Agree

S/N	STATEMENT	1	2	3	4	5
1	The organization has adopted strategies that influence employees to comply with the information security requirements					
2	A reward is one of the main strategies employed by my organization to ensure compliance with information security policies					
3	The reward for Information Security Policy (ISP) compliance is very well enforced					
4	Punishment is one of the main strategies employed by the organization to ensure compliance with information security policies					
5	The punishment for non-compliance with Information Security Policy (ISP) is very well enforced					
6	If I comply with information security policies, I will get a material reward					
7	If I comply with information security policies, I will get an appreciation					
8	If I comply with information security policies, I will get acknowledgment from my superior					
9	If I comply with information security policies, I will get a promotion.					

10	If I do not comply with information security policies, I will get punished or demoted					
11	If I do not comply with information security policies, I will receive a personal reprimand in oral or written assessment reports					
12	If I do not comply with information security policies, I incur monetary or non-monetary penalties					
13	The organization disciplines employees who break information security rules					
14	The organization terminates employees who repeatedly break security rules					
15	The information I deal with in my daily work is such that it is imperative to ensure confidentiality and maintain privacy.					
I comply with the organization's Information Security Policies Requirements because:						
16	I feel morally obligated to comply with the organization's ISP					
17	I feel guilty if I do not comply with the organization's ISP					
18	It is favorable to me					
19	It is realistic and makes work flexible					
20	It helps to achieve the organization's goals					
21	It enhances my performance					
22	It addresses my concerns in respect of the existing ISP					
23	It protects the organization's information systems					
I don't comply with the organization's Information Security Policies Requirements because:						
24	It is not favorable to me					
25	It is unrealistic and rigid					
26	It delays work/stills performance					
27	It holds me back from doing my actual work					

28. If the organization adopts reward strategies to ensure compliance, what is the degree of its influence on the employees' compliance with the information security measures?

    Very High [ ] High [ ] Low [ ] Very Low [ ] No Influence [ ]

29. If the organization adopts punishment strategies to ensure compliance, what is the degree of its influence on the employees' compliance with the information security measures?

    Very High [ ] High [ ] Low [ ] Very Low [ ] No Influence [ ]

Part 3

EFFECTS OF ISP BREACHES ON REVENUE

This part is meant to find out the effects of information security breaches on the organization's revenue. Please, indicate your agreement, disagreement, or knowledge on each of the questions by ticking [√] the appropriate box that corresponds to each question.

1= Strongly Disagree 2= Disagree 3= Neutral 4= Agree 5 = Strongly Agree

S/N	STATEMENT	1	2	3	4	5
1	The company has never recorded an incident of information security breaches.					
2	Frequent occurrence of information security breaches in the organization can severely affect the income of the company?					
3	The company has lost some customers in the past years due to information security breaches.					
4	The organization has lost some investors due to information security breaches.					
5	The organization has spent a relatively huge sum of money replacing computer software due to virus attack					

6	The organization has spent money to hire experts to manage its information resources after security breaches					
7	The company has spent a huge sum of money on other postattack remedies.					
8	The organization has paid money to compensate customers due to Information Security breaches					
9	The organization has faced legal actions before because of breaches in its information security resources					
10	There was a reduction in sales because Customers complained that they were not able to access our website or any of our platforms.					
11	Breaches in the information resources are inconsequential to the capital growth of the organization.					
12	The organization has lost money in the past due to illegal access to its bank details					
13	The impact of the information breaches on the organization is insignificant					
14	The organization will lose its competitive power when Secret ingredients and process of manufacturing of our products are released to outsiders					
15	The organization spent a relatively huge sum of money replacing salient files because most of our computers were infected with a virus					
16	The organization has experienced information security breaches before but they didn't have any severe impact on production and sales					
17	The organization has experienced information security breaches before but its impact on production and sales was not noticed					
18	The organization has experienced information security breaches before and the organization recorded a loss for that accounting year					