The Influence of Organizational Culture on Information Security Policy Success

George Tetteh Hadjor
Emmanuel Kwasi Gadasu
2014

Master of Science (120 credits)
Computer Science and Engineering

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering
“In most organizational change efforts, it is much easier to draw on the strengths of the culture than to overcome the constraints by changing the culture”.

Edgar Schein, professor MIT Sloan School of Management
Abstract

It is generally accepted that the protection of the organization’s information assets begins with the creation of information security policies and it is these that serve as a blueprint against which the success of all information security efforts are hinged (Whitman and Mattord, 2009). Key to the success and effectiveness of these policies is human behaviour better still known as the human factor, which is described as the weakest link in information security (Mitnick et al. 2002). This assertion is also confirmed by Schneier (2000) who mentions that information security is only as good as its weakest link, and people are the weakest link in the chain.

Every cultural setting (be it in an organization or other societal grouping) has particular values, beliefs and practices that it shares as part of its identity and it is these characteristics that largely influence the behaviours of the members. This assertion is confirmed by Triandis et al. (2002) who state that personality is shaped by both genetic and environmental influences but that the most important of the latter are cultural influences. Maccoby (2000) also tells us that personality emerges under the influence of both genes and environment but Loughling & Barling (2001) argue more emphatically that values, beliefs and attitudes significantly influence our behavior. Schein (2004) in his definition reveal that the collection of values, beliefs, practices and assumptions held by people in an organization, which are usually taken for granted, is what defines the organization’s culture.

The objective of this research is to investigate the role that this culture (within organizations i.e. organizational culture) may have on the successful implementation of information security policies. The idea is to explore how organizational cultural characteristics can positively influence human behaviour which will then positively impact on information security policy success. If these particular organizational cultural traits are found to positively influence normative human behaviour and hence the successful implementation of information security policies, they can be adapted and/ or adopted by other organizations as part of their organization’s culture to increase their rate of success with security policy implementation.

It is our belief that an approach to security policy implementation that is attended to from the organizational culture perspective (other than just security awareness or the use of security technology) has a higher rate of success because the culture of the organization, like the information security policy is founded on the mission/vision of organization. We will carry out this research by exploring the organizational culture of UNICEF Ghana against the backdrop that they have been successful with the implementation information security policies.

Keywords: Information Security, Information Security Policy, Information Security Policy Implementation, Organizational Culture, Cultural Characteristics, Information Security Culture
Preface

This thesis is submitted to the Department of Computer Science, Electrical and Space Engineering at Lulea University of Technology, in partial fulfillment of the requirements for a Master's Degree in Information Security.

This research work was initiated in December 2012 and completed in June 2013 under the supervision of Dan Harnesk (PhD), of the Department of Computer Science, Electrical and Space Engineering at Lulea University of Technology. The research work was jointly undertaken by both authors (George Tetteh Hadjor and Emmanuel Kwasi Gadasu) who equally contributed to all portions of the research.
Acknowledgement

We are highly indebted to our supervisor, Dan Hanersk (PhD) of the Department of Computer Science, Electrical and Space Engineering at Luleå University of Technology. He was instrumental in assisting us shape the research topic and also stringent in guiding us throughout the research process.

We extend our gratitude to the UNICEF Ghana country office for allowing us use their organization and its employees for carrying out our empirical studies in this research, most particularly the Chief of Operations; Mahesh Adhikari for granting us unlimited access to talk to him.

We also appreciate the company of our brother and study partner; Henry Lambert Quist who dutifully stayed with us late in the nights and also provided us with insights and perspectives on our research.
Contents

Abstract ........................................................................................................................................... 2

Preface ............................................................................................................................................ 3

Acknowledgement .......................................................................................................................... 4

Contents .......................................................................................................................................... 5

Figures ........................................................................................................................................... 9

Tables ........................................................................................................................................... 10

1 Introduction .................................................................................................................................. 11

1.1 Background ............................................................................................................................... 11

1.2 Motivation and Call for Solutions ............................................................................................. 12

1.3 Problem Situation ...................................................................................................................... 12

1.4 Research Objective .................................................................................................................. 13

1.5 Research Question ................................................................................................................... 13

1.6 Expected Results and Significance of Study ............................................................................. 13

1.7 Assumption ............................................................................................................................... 13

1.8 Scope ....................................................................................................................................... 14

2 Literature Review - Areas of Concern ......................................................................................... 15

2.1 Information Security .................................................................................................................. 15

2.2 Information Security Policy ...................................................................................................... 15

2.3 Information Security Policy Implementation ............................................................................. 16

2.4 Challenges to information security policy Implementation ....................................................... 17

2.5 Behavioral Factors and Information Security Policy Implementation .................................... 18
2.6 Culture .................................................................................................................19
2.7 Organisational Culture: Shared Values et al. .........................................................20
2.8 Dimensions of Culture ........................................................................................22
2.9 Dimensions of Organizational Culture .................................................................23
2.10 Organizational Culture & Employee Behaviour..................................................25
2.11 Organizational Culture, Information Technology & Performance ......................25
3 Framework of Ideas ...............................................................................................27
  3.1 Information Security Policy Process Model .........................................................27
  3.2 The Organizational Culture Framework ..............................................................28
  3.3 Framework of the Relationship between Organizational Culture (OC) and Information Security Culture (ISC) .........................................................................28
  3.4 Schein’s Three Levels of Culture .........................................................................31
  3.5 Bringing the Theoretical Ideas Together ..............................................................32
  3.6 Theoretical Proposition .......................................................................................33
    3.6.1 Management Style ..........................................................................................34
    3.6.2 Trust & Responsibility ..................................................................................34
    3.6.3 Bureaucracy & Dependencies ......................................................................35
    3.6.4 Motivation ....................................................................................................35
    3.6.5 Budget and Funding ....................................................................................35
    3.6.6 Awareness, Education and Training .............................................................36
    3.6.7 Participation & Coopération .........................................................................37
    3.6.8 Commitment ..................................................................................................37
3.6.9 Communication............................................................................................................. 37
3.6.10 Supervision, Co-ordination & Control ...................................................................... 38

4 Research Approach and Design.......................................................................................... 39
  4.1 The Research Approach...................................................................................................... 39
  4.2 Case Study as a Research method...................................................................................... 39
  4.3 The Case Study Design....................................................................................................... 40
  4.4 Case Organization Selection.............................................................................................. 40
  4.5 The Research Journey........................................................................................................ 41
    4.5.1 Literature review ........................................................................................................ 41
    4.5.2 The Research Process.................................................................................................. 41

5 Data Collection and Analysis............................................................................................... 43
  5.1 Data Collection Strategy.................................................................................................... 43
  5.2 Mode of Enquiry................................................................................................................ 44
  5.3 Background of Case Organization..................................................................................... 44
  5.4 Participant Observation...................................................................................................... 45
  5.5 Document Analysis........................................................................................................... 46
  5.6 Interviews.......................................................................................................................... 46
  5.7 Data Analysis Strategy....................................................................................................... 47

6 Results & Findings ............................................................................................................... 49
  6.1 Overall Findings: Per Data Sources.................................................................................. 49
    6.1.1 Participant Observation............................................................................................... 49
7.2 Conclusion..................................................................................................................72

7.3 Further Research ........................................................................................................73

7.3.1 Why Implementation and not compliance...............................................................73

7.4 Steps to Achieving Success with policy Implementation............................................74

7.5 Limitations..................................................................................................................74

8 References ..................................................................................................................75

Appendix A: Interview Guide ..........................................................................................81

Appendix B: Extracts of UNICEF Competency Framework Definitions and Behavioral
Indicators.........................................................................................................................85

Figures

Figure 2.1 – Hofstede’s Three Levels of Uniqueness in Human Mental Programming ------19

Figure 2.2 – Hofstede’s Onion Diagram ........................................................................20

Figure 2.3 – Schein’s Three Levels of Culture.................................................................21

Figure 3.1 – Knapp et al.’s Information security Policy Process Model..........................27

Figure 6.1 – Top Level Hierarchy of UNICEF’s Shared (N) Drive....................................61
Tables

Table 2.1 – Hofstede’s Six Dimensions of National Culture

Table 2.2 – Hofstede’s Six Dimensions of Organizational Culture

Table 2.3 – Detert et al.’s Eight Dimensions of Organizational Culture

Table 3.1 – Framework of the relationship between Organizational Culture and Information Security Culture.

Table 5.2 – Interview Table

Table 6.1 – Communication Competency extract from the UNICEF Competency Framework
1 Introduction

A sound information security policy is the basis for a successful information security program. This notwithstanding, a number of factors comes into influence the successful implementation of the policies. Key among them is senior management commitment, availability of funds, business objectives, the appropriate technology architecture and the right organizational culture (Knapp et al., 2009). To achieve success with information security policies, it is therefore extremely important to attend to these requirements. This research focuses on how organization culture can successfully influence an information security policy

1.1 Background

Whitman & Mattord (2009) define policy as a plan of action used to convey instructions from the organization’s senior management to those who make decisions, take and perform certain actions. This is akin to ISO/IEC’s (2005) definition that the objective of policy is to provide management direction and support for information security in agreement with business requirements and relevant laws and regulations. In Information Security (IS), policies are especially important because they serve as the blueprint for the overall security program and create a platform to implement information security practices in an organization (Whitman et al, 2009).

A majority of security incidents are caused by internal personnel in organizations intentionally or unintentionally through the violation of IS policies (Whitman and Mattord 2009). To make a policy effective and enforceable, Whitman and Mattord (2009) defined a number of criteria to meet this objective including the policies dissemination, comprehensions, review, compliance and uniform enforcement. Similarly other researches in their bid to ensure successful implementation have posited a number of such strategies (Tryfonas et al., 2001; and Dhillon, 1999 etc.).

Many similar guidelines have been espoused to ensure that policies are properly developed and implemented. This goes to confirm that a security policy is of no value unless it has been implemented well and the organization is operating under its guidelines and directions.

Over time however, we have gotten to the point where the technical requirements for policy development are being adhered to but policies still continues to fail. There is much advice as to how to successfully implement information security policies but one of the most important, yet least discussed aspects is the role that organizational culture has to play in its effective execution. The human factor is one area that continues to be drummed home as a major challenge in information security implementation with it being described as the weakest link in the information security domain, Schneier (2000, see Sasse et al, 2001). By and large, the behaviour of employees (and their attitude to security) in an organization are predominantly influenced by the organization’s culture. If the security culture of an organization is lax, policy more or less doesn’t surf beyond the print and ink of the policy documents.

According to Knapp et al (2009), in addition to numerous processes that shape the development of policy, a number of factors (internal and external) exist that have the potential to influence an organization’s information security policies. The model they posit espouses five internal influences including internal security threats, senior management support, business objectives, technology architecture and organizational culture, which is the focus of this study.

Schein (1996) is credited for postulating the contemporary definition of organizational culture and he defines culture as a set of behavioural and cognitive characteristics. He also goes on to further explain that organizational culture is the basic beliefs and assumptions shared by the organizational members that have worked well enough to be considered valid and therefore to be transferrable to new members. Researchers such as Dhillon (1997), Lim et al (2009), Ruighaver et al. (2007) Von Solms, R. & Von Solms, B.(2004) have also called for a look at the totality of behaviour that will contribute to protecting the organization’s information. Detert et al. (2000) see Organizational
culture as a driver for organizational innovation and performance. To bring success to information security policies, there is therefore a need to explore the use of this organizational culture as a vehicle to drive home the requirements of information security policies.

1.2 Motivation and Call for Solutions

As revealed by IS research, the human factor was largely ignored as a way to tackle information security with the focus being on technology security solutions (Dhillon & Torkzadeh, 2006). However with the current focus on the human factor as a way to tackle information security, the focus has been on information security awareness as a way to direct and influence the behaviour of employees in the organization. However a more powerful and latent approach that is already known but overlooked is the use of organizational culture to influence and stimulate appropriate employee behaviour towards successful execution of information security policy. An organization’s culture is an already existent resource and the way forward is to identify particular cultural traits that can be adapted to benefit a successful information security policy.

We are motivated by this opportunity to find an easier, cheaper and less prohibitive solution to the problems information security policy implementation and information security in general.

Among the many challenges that confront security policy implementation (senior management support, technology architecture, budget etc.), the influence of organizational culture although overt, seem to have been side-lined and given little attention. There is therefore a need to look in this direction as a possible “panacea” to achieve success with information security policy. As revealed by Huebner et al. (2006, see Albrechtsen, 2006) there exist few papers that focus on the behavioral and social aspects of information security although the challenge is to control human behaviour.

1.3 Problem Situation

Information security continues to fail primarily because of the failure of information security policies. This is because information security policies are the necessary foundation for all security programs in an organization (Knapp et al, 2009). The failure of the information security policies can be traced among other reasons to implementation challenges of which the attitudes of employees is key (Knapp et al, 2009). This is notwithstanding the many legal, administrative, and political guidelines that have been used in shaping policy development to make it effective (ISO 17799, Whitman & Mattord, (2009)).

According to Leach (2003, See Lim et al (2009)), the Information Security Forum (November 2000) also reports that as many as 80% of major security failures could be as a result of poor security behaviour by staff instead of poor security solutions. Work by (Pahnila, Siponen & Mahmood, 2007, workman et al., 2008, see Lim et al, 2009) suggest also that major threats to information security is caused by careless employees who do not comply with the organization’s policies and procedures.

As revealed by Knapp et al. (2009), in addition to other requirements, the right organizational culture remains one of the main pillars to achieving a successfully implementing an information security policy.

By this extension, a lack of appropriate organizational culture remains one of the main challenges to achieving success with information security policies.
1.4 Research Objective

The focus of this study is not to research explicit ways to solve the human factor problem to information security such as with modest information security awareness and the use of mechanistic compliance controls. It is to investigate relevant organizational culture that can be utilized to implicitly influence and motivate employee behaviour for the successful implementation of information security policy and information security as a whole.

Overall we hope to achieve the below objectives at the end of the study:

- Highlight and sensitise policy formulators and senior management on the impact that organizational culture has on information security policy and information security success as a whole.
- Investigate and bring to the fore particular organizational cultural characteristics that can be cultivated by organizations to increase their success with information security policies.
- Set the basis for other researchers to investigate ways to adapt/adopt the identified organizational cultural characteristics to improve upon the success of Information security policies.

1.5 Research Question

The overarching question with regards to this study is

- What is the role of organizational culture in the successful implementation of Information Security Policies?

To answer this question a number of embedded questions need to be asked, analysed and answered and these include:

- What factors influence a successful information security policy
- In what ways does organizational culture influence information security policy?
- What characteristics define this organizational culture?

1.6 Expected Results and Significance of Study

It is expected that the research will come up with particular organizational cultural characteristics that can implicitly stimulate employees to behave in ways that are congruent to prudent security behaviour. If these practices are identified and confirmed, it can be adapted and/or adopted by other organizations to improve upon their information security policy success so they move away from cost prohibitive security approaches such as effecting mechanistic controls aimed at orienting and directing employee behaviour.

1.7 Assumption

The basic assumption for this research is that organizational culture is the principal requirement for the successful implementation of an information security policy. The research also assumes that the organization of study is information technology enabled, has developed and implemented information security policies as part of its information security program and has achieved some level of success with the policy’s implementation. The third assumption is that the organization is sizeable and old enough to have developed some kind of organizational culture which it uses to work towards the achievement of its objectives.
To validate this research, the prime supposition is that the organization of study is successful with information security policy implementation. This success should be manifested in the low number of information security incidents and the high level of employee compliance with information security rules and requirements.

1.8 Scope

The focus of this study is on information security policy implementation and ways to improve on the success rate from the perspective of organizational culture only. It will neither wade into technical factors nor other human factor approaches such as the study of individual values and beliefs to improve on success rate. The focus is on the shared cultural values, beliefs and practices held and lived by the organizations as a whole and its relation to IS policy implementation success. The study will focus on UNICEF Ghana and its organizational cultural characteristics under the assumption that it has been successful with implementing information security policies.
2 Literature Review - Areas of Concern

Whilst carrying out this study, we have reviewed various areas of knowledge ranging from social science, psychology to information security in order to develop a suitable theoretical proposition for undertaking the exploratory journey and answering the research questions.

2.1 Information Security

ISACA (2012) defines Information security as “something that ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability).”

Yulia et al (2012) also similarly defined information security as the actions taken in advance to prevent undesirable events from happening to the knowledge, data and its meaning so that knowledge, data and its meaning can be relied upon. They developed this definition for information security from the English Dictionary meaning of information (computing): the meaning given to data by the way in which it is interpreted and security as the state of being secure or precautions taken to ensure against theft, espionage etc.

Early research in the field defined information security around the classic security objectives of confidentiality, integrity and availability, often referred to as the CIA triad (see e.g. Gollman, 1999; Jonsson, 1995, ISO/IEC 17799, 2005). Other researcher such as Donn Parker in his Parkerian Hexad rule augments the objectives to include possession, utility and authenticity (Kabay, 1998) whilst Whitman & Mattord (2009) add accuracy to parker’s six objectives.

Owing to current threats, challenges and changing security landscape, the new direction concerns defining information security in a broader perspective that will address social groupings and the behaviour of people (Dhillon, 1995). Dhillon & Backhouse (2000) for example suggest complementing the CIA with Responsibility, Integrity, Trust and Ethicality (RITE), arguing that the CIA definition was restrictive and applied only to information seen as data. Dhillon and Torkzadeh (2001, see Kolkowska, 2003) also claim that because values guide human behaviour, actions and determine feelings and beliefs, which consequently determines the organizations where they work, the management of information security in organizations should begin with values.

2.2 Information Security Policy

According to the American Heritage Dictionary (2000, see von Solms and von Solms (2004), a policy is defined as (1) “a course of action, guiding principle, or procedure considered expedient” or (2) “a certificate of insurance”.

According to Hone and Eloff (2002, see Knapp et al., 2009), information security policy is undoubtedly, the singularly most important of information security controls. They go on to define the information security policy as a plan identifying the organization’s vital assets together with a detailed explanation of what is acceptable, unacceptable employee behaviour in order to ensure security of information. This is similar to the position of Whitman and Mattord (2009), who state that the core objective of any policy is to influence and determine the decisions, actions and behavior of employees by specifying what behaviour is acceptable and unacceptable. In explaining this, Fung et al (2003) stated that an information security policy is the keystone of good information security management.

From their perspective, Whitman and Mattord (2009) disclose that the protection of the organization's information assets; information security, begins with the creation of information security policies and it is this that serves as a blueprint against which the success of all information security efforts is hinged.
In their explanation, Tryfonas et al (2001, see Al-Awadi et al, 2007) chose to see an information security policy as a combination of principles, regulations, methodologies, techniques and tools established to protect the organization from threats. But Canavan (2003), also reveal that information security policies also help organizations to identify its information assets and define the corporate attitude to these information assets. The position of Canavan (2003) is further supported by Davis and Olson (1985, see Knapp et al., 2009) who define policy in a planning and control context with the main purpose of establishing the limits of employee behaviour among other. The reason why policy exists according to Dancho (2003, see Talbot and Woodward, 2009) is to document the security requirements of the organization and explain the responsibilities of employees and the need for security.

Security driven by technology rather than policy is an inadequate means of protecting information, and will likely not be in line with the business aims of the organization, (Talbot and Woodward, 2009). Even where security has been driven by policies, there is a history where the ignoring of the policies by employees in an organization remains a challenge (Talbot and Woodward, 2009).

### 2.3 Information Security Policy Implementation

Once policy has been created, perhaps the hardest part of the process is rolling it out into the organization, InstantSecurityPolicy (2008). This position is supported by Whitman and Mattord (2009) who reveal that “notwithstanding the fact that policies are the least expensive control to execute, they are the most difficult to implement properly.”

Implementation literally means carrying out, accomplishing, fulfilling, producing or completing a given task (Paudel, 2009). According to Paudel (2009), the founding fathers of implementation, Pressman and Wildavsky (1973) define it in terms of a relationship to policy as laid down in official documents and it may be viewed as a process of interaction between the setting of goals and actions geared towards achieving them. Fixsen et al (2005) similarly define implementation as a “specified set of activities designed to put into practice an activity or program of known dimensions”. They go on to say that implementation processes are purposeful and the activity or program being implemented is described in such a way that independent observers can detect its presence and strength.

Paudel (2009) theorizes that “implementation can be conceptualized as a process, output and outcome; this process is a series of decisions and actions directed towards putting a prior authoritative decision into effect”. He explains further that the essential characteristic of the implementation process is the timely and satisfactory performance of certain necessary tasks related to carrying out of the intent of the policy. As an alternative he suggests that implementation can also be defined in terms of output or extent to which policy goals have been satisfied. He finally concludes that, at highest level of abstraction, implementation outcome implies that there has been some measurable change in the larger problem that was addressed by the policy.

Policy implementation encompasses those actions by individuals or groups that are directed at the achievement of objectives set forth in the policy (Paudel, 2009). According to Whitman and Mattord (2009), during the implementation phase, the organization translates its blueprint for information security into a concrete project plan. The project plan then delivers instructions to the individuals who are executing the implementation. Hermans (2010) reveal that literal implementation of policies is rare, because it is virtually impossible. He goes on to say that the conception that implementation is a mere translation of policies and strategies into reality, which can be done in a mechanistic manner, is flawed.

To this, Paudel (2009) suggests that implementation inevitably takes different shapes and forms in different cultures and institutional settings, a position supported by Barman(2001, see Al-Awadi et al, 2007) who argues that the content of the information security policies may vary from one organization to other but that all policies have some topics in common.
In their research, Al-Awadi et al (2007) reveal that during their interviews, it came out that, “Performance of the organization will be successful when we create a policy, effectively implement it, it is accepted by employees, and stick to our rules and don’t manipulate them”. Canavan (2003) explains that the information security policy can only be enforced by means of implementation. When an organization puts an information security policy into practice, employees can be requested to follow the rules and be made aware of their rights and responsibilities Hone and Eloff (2002).

According to David (2000, see Knapp et al, 2009) policy must be enforced to make it effective and the aim is to change the habits of employees in the organization. A host of researchers (Canavan (2003); Doherty and Fulford (2005); Hone and Eloff (2002); Salter et al (1998); Madigan et al (2004); Tryfonas et al (2001); Dhillon (1999), see Al-Awadi et al, 2007) indicate that organizations should consider a number of criteria in order to implement information security policies effectively. These include, “the policy must: fit the organizational culture; have a style which is consistent with the organization’s general communication style; not read like a technical document, but use simple language to ensure it is not difficult to understand; be effective and dynamic; use a concrete language rather than abstract language; specify the job responsibilities; state the purpose of the policy and the scope of the organization; and explain what activity is acceptable and what is not”.

Elmore (1978, see Paudel, 2009) also identified four main ingredients for effective implementation, these include “(1) clearly specified tasks and objectives that accurately reflect the intent of policy; (2) a management plan that allocates tasks and performance standards to subunits; (3) an objective means of measuring subunit performance; and (4) a system of management controls and social sanctions sufficient to hold subordinates accountable for their performance”. Elmore (1978) concludes that failures of implementation are, by definition, lapses of planning, specification and control.

In the course of their study particularly during interviews, Al-Awadi et al (2007) mention that some experts have said that the organization's clear goals and objectives are essential in implementing information security policies and that having a culture of secure information in the organization will affect its success.

The issues identified with IS policy implementation is affecting the effectiveness of the policies and the information security which the implementation is intended to provide says Talbot and Woodward (2009).

2.4 Challenges to information security policy Implementation

Whitman and Mattord (2009) tells us that there are aspects to information security implementation that are non-technical and relate to human nature and behaviour. This assertion is supported by Rosenbaum (1986, see Dalton et al 2007) who discloses that implementation failure occurs when the policy theory is sound but not properly put in place. He reveals that some reasons for implementation failure include lack of resources, inexperienced personnel, and insufficient training. Implementation failure can also relate to the extent to which the implemented policy conforms to the original plan or when there is a lack in quality adaptation Durlak and DuPre (2008, see Wandersman et al 2005).

Pressman and Wildavsky (1984, see Hermans, 2010) reveal that policy is complicated by the fact that it involves multiple actors (employees) and all these actors have to make their own choices as to how to implement their portion of the policy. They go on to explain further that these actors will do what they think needs to be done and they also choose which activities involved in the implementation they should pursue or neglect. This point is buttressed by Whitman and Mattord (2009) who explain that apart from changes in procedure, hardware, software and data, the implementation phase can only be fully accomplished if this change also involves people.
Paudel (2009) in discussing his three generations of policy implementation explains that the top-down approach “exhibits a strong desire for ‘generalizing’ policy advice and this requires finding consistent and recognizable patterns in behaviour across different policy areas”. He however mentions that the approach largely restricts the actors involved in the policy implementation. He also goes on to say that this approach emphasizes formal steering that leads to centralization and control. The interest of this approach therefore is directed toward issues such as funding, formal organization structure and authority relationships. In discussing the bottom-up approach, Paudel (2009) explains that the focus of this approach is the formal and informal relationships in the policy’s environment with the focus being on individuals and their behaviour. He however reveals that the failure of this approach emerges from the inappropriate decisions, flawed routines and personal malfunctions.

In explaining their Information Security policy process model, Knapp et al (2009) reveals that the policy stages of approval, awareness and training and implementation are affected by a number of internal factors. These five internal influences are senior management support, business objectives, internal threats, technology architecture and organizational culture. In explaining the last influence, he mentions that security is a management problem and the culture of the organization reflects how management handles and treats security problems. He further iterated that organizational culture predominantly determines the overall employee attitude towards security. To buttress his point, he cites an example where if an organization’s culture is hostile towards a security policy that the employees perceive as unreasonable, the security staff will face difficulty with achieving compliance for that policy.

According to Talbot and Woodward (2009), quite a number of issues can be identified as confronting the policy implementation process, policy effectiveness and information security in general. They list these challenges as; (1) a culture of ignoring policies; (2) minimal policy awareness (3) minimal policy enforcement; (4) lack of a compliance framework; (5) ad hoc policy update and review; (6) no formal non-compliance reporting; (7) a lack of policy framework; (8) lengthy policy approval and development process; (9) apparent inconsistency enforcement across the whole organization.

2.5 Behavioral Factors and Information Security Policy Implementation

Following up from the discussion of the previous section, one realizes that to overcome the cultural challenges discussed, there are a number of behavioral traits that need to be held or exhibited by employees to make the security policy implementation successful.

In their discussion of the project implementation plan for implementing an information security project, Whitman and Mattord (2009) discussed a number of relevant points that need to be attended to and these include, the time and schedule considerations, assignment of tasks and staffing, the amount of effort required to carry out the project, the financial and budgetary considerations, task dependencies, training and indoctrination, and supervision.

In the discussion of critical success factors to information security implementation, the ISO17799 standard discusses eight such factors. These include (1) security policy, objectives and activities that properly reflect business objectives; (2) clear management commitment and support; (3) proper distribution and guidance on security policy to all employees and contractors; (4) effective ‘marketing’ of security to employees (including managers); (5) provision of adequate education and training; (6) a sound understanding of security risk analysis, risk management and security requirements; (7) an approach to security implementation which is consistent with the organization’s own culture; (8) a balanced and comprehensive measurement system to evaluate performance in IS management and feedback suggestions for improvement.

Yanus and Shin (2007) also similarly elicit a number of indicators that should be used to evaluate an information security awareness program, these include: (1) sufficient funding to implement an agreed
upon strategy; (2) appropriate organizational support to enable employees with key responsibilities such as CIO, program officials, information security program managers; (3) support for broad distribution and posting of security awareness items; (4) executive/senior level messages to staff regarding security; (5) use of metric for a decline in security incidents and violations, the gap between existing awareness and training coverage, the percentage of users being exposed to awareness material, the percentage of users with significant security responsibilities being appropriately trained; (6) level of attendance at mandatory security forums/briefings; (7) recognition of security contributions; (8) motivation demonstrated by employees playing key roles in managing and coordinating the security program.

2.6 Culture

Hofstede, the well-known pioneer in cross-culture groups and organizations (Wikipedia, 2013) defines culture as “the collective programming of the mind which distinguishes the members of one group or category of people from another”, Hofstede (1993). He further explains that it is a collective phenomenon, because it is at least partly shared with people who live or lived within the same social environment, which is where it was learned. He goes on to differentiate culture from personality and human nature with the explanation that human nature is inherited, culture is learnt, but personality is both learnt and inherited. See figure below

Figure 2.1 – Hofstede’s Three Levels of Uniqueness in Human Mental Programming

Kluckhohn (1954, see Triandis et al, 2002) also analogizes culture to society just as memory is to individuals. He explains that culture includes what has worked in the experience of a society, so that it is worth transmitting to future generations. This is later corroborated in Schein’s (2004) definition of culture as “values, beliefs and assumptions that a group of people share”. Triandis et al (2002) also similarly explains that elements of culture are shared standard operating procedures, unstated assumptions, tools, norms, values, habits about the sampling environment and the like. Hofstede (1993) however reveals that cultural differences manifest themselves by way of symbols, rituals, heroes and values. Symbols are words, pictures gestures or objectives that carry particular meaning with the culture; heroes are persons with highly prized characteristics who serve as models for behaviour; rituals are a collection of activities that are technically superfluous but socially essential and are therefore performed for their own sake. He further explains that symbols, rituals and heroes can be subsumed
under the term practices (visible with meaning lying in the way they are perceived by insiders) but values (invisible and manifested in alternatives of behaviour) lie at the core of culture (Hofstede, 1990).

![Hofstede's Onion Diagram](image)

**Figure 2.2 – Hofstede’s Onion Diagram**

2.7 Organisational Culture: Shared Values et al.

All organizations have values whether articulated or not. However as noted by O’Reilly et al (1991), what senior management say must be done is different from what they actually do. This tells us that the values that an organization espouses are not what are actually lived. This fact is confirmed by Schein (2004) for which reasons he calls for looking at the historical values, beliefs and assumptions of key leaders and founders. Shared values are regarded as fundamental to the idea of a strong unitary culture (Murphy and McKenzie, 2002). Dhillon and Torkzadeh (2006) also claims that “because values guide human behaviour, determine and guide actions, feelings and beliefs and consequently determine the organizations where they work, the management of information security in organizations should begin with values”.

Edgar Schein is perhaps one of the most authoritative researchers in the field of organizational culture. He formally defines culture as “the basic assumptions that a given group has invented, discovered or developed in learning to cope with its problems of external adaptation and internal integration and that have worked well enough to be considered valid and therefore, to be taught to new members as the correct way to perceive, think and feel in relation to problems”, Schein (1984). With his research mainly against the backdrop of the organization, he further argued that what really drives daily behaviour is the learned, shared tacit assumptions on which people base their view of reality.

This he says includes “what is valued; the dominant leadership styles, the language and symbols, the procedures and routines; the definitions of success that characterizes the organization; the habit of thinking; people’s mental modes; the climate and the group norm”.


In his organizational culture and leadership publication, Schein (2004), reveals that “the meaning of culture has been oversimplified with the temptation to conclude that culture is just, the way we do things around us, the company climate, the reward systems, our basic values” and so on. This revelation he explains are however only manifestations of culture and that culture actually exists at three levels moving from the very visible to the very tacit and invisible.

**The Three Levels of Culture**

- **Artifacts**: Visible organizational structures and processes (hard to decipher)
- **Espoused Values**: Strategies, goals, philosophies (espoused justifications)
- **Underlying Assumptions**: Unconscious, taken for granted beliefs, perceptions, thoughts, and feelings... (ultimate source of values and action)

**Figure 2.3 – Schein’s Three Levels of Culture**

The first level deals with the artifacts i.e. what you see, hear or feel when you are in the environment of an organization. The second level, Schein (2004) explains are the espoused values of the organization that are supposed to create a certain image of the organization. They are what ought to be, Gordon (1991, see McKenzie (2010)). This level of espoused values is supposed to explain the artifacts of the first level but sometimes there are inconsistencies that call for one to seek for deeper understanding. This brings us to the third level which requires that one takes a historical view of the values, beliefs and assumptions of the key leaders and founders of the organization. This is so because organizations are founded by individuals or small teams who initially impose their beliefs, values and assumptions on the initial people they hire. The assumptions at this level are those things which are commonly taken for granted as “correct” within the organization, Gordon (1991, see McKenzie (2010)).

Schein (2004) deduced that “the essence of culture is the jointly learnt values and beliefs that work so well that they are taken for granted and non-negotiable”. Simply put, what employees will call “the way we do things around here” although he reveals that the underlining assumptions of this statement are difficult to reconstruct. This is corroborated by Cook and Szumal (2000) who also define organizational culture as common assumptions, values and beliefs shared by its members, which define how individuals think and behave in an organizational setting. Hofstede (1998) similarly refers to it as “the collective programming of the mind which distinguishes members of one organization from another”. He goes on to explain that organizational culture is a characteristic of the organization and not individuals.
Schein (2004) also differentiates between espoused values and underlying assumptions. He cites an example, “where an organization’s espoused theory may be that it takes individual needs into consideration in making geographical moves; yet its “theory-in-use” may be that anyone who refuses an assignment is taken off the promotional list”.

Schein (2004) goes on to conclude that to really understand culture, one needs a process to systematically observe and talk to insiders to make the assumptions explicit. He however also reveals that as an organization grows, the important elements of the culture are deeply embedded in the structure and major processes including its ideologies and philosophies.

### 2.8 Dimensions of Culture

To study the cultural influence on societies (including organizations), one needs typologies (Schein, 1985) or dimensions (Hofstede, 1980) for analyzing the behaviors, the actions and the values of their members, Pheng et al (2002). In 1952, U.S. anthropologist Clyde Kluckhohn (1962) argued that there should be universal categories of culture and a number of researchers have followed suit to categorize culture based on a number of criteria (Hofstede, 2011). Among the notable researchers, Hofstede carried out a cultural values survey of people in over 50 countries around the world, working with the local subsidiaries of one large multinational firm- IBM (Hofstede, 1993). He identified six different dimensions of national culture which he warns are different from the six dimensions of organizational culture and should also not be confused with value differences at the individual level (Hofstede, 2011). These six dimensions of national culture include (1). Power Distance: related to the different solutions to the basic problem of human inequality; (2). Uncertainty Avoidance: related to the level of stress in a society in the face of an unknown future; (3). Individualism versus Collectivism: related to the integration of individuals into primary groups; (4). Masculinity versus Femininity: related to the division of emotional roles between women and men; (5). Long Term versus Short Term Orientation: related to the choice of focus for people's efforts: the future or the present and past.(6) Indulgence versus Restraint: related to the gratification versus control of basic human desires related to enjoying life (Hofstede, 2011).

<table>
<thead>
<tr>
<th>Hofstede’s Six Dimensions of National Culture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Distance</td>
</tr>
<tr>
<td>Uncertainty Avoidance</td>
</tr>
<tr>
<td>Individualism</td>
</tr>
<tr>
<td>Masculinity</td>
</tr>
<tr>
<td>Long term</td>
</tr>
<tr>
<td>Indulgence</td>
</tr>
</tbody>
</table>

**Table 2.1 – Hofstede’s Six dimensions of National Culture**
Indeed, Hofstede et al (1990)’s data show that the different organizations within the same national culture could be distinguished from the behavioural norms (day-to-day practices) they differently adopt and not from their values (Delobbe et al, 2002). Hofstede himself acknowledges that "the dimensions of national cultures are not relevant for comparing organizations within the same country". In contrast with national cultures, embedded in values, organizational cultures are embedded in practices (Wikipedia, 2013).

2.9 Dimensions of Organizational Culture

The organization provides the shell within which national and professional cultures operate and is a major determinant of behaviour (Helmreich, 1999). National and organizational cultures are phenomena of different orders and using the term “cultures” for both is in fact somewhat misleading (Hofstede, 1990). Hofstede (2011) argues that changing the level of aggregation studied changes the concept of culture; and goes on to reveal that organizational culture is what is acquired and exchangeable when people take on a new job. Hofstede, together with his research colleagues collected data in twenty work organizations in two countries where they identified six independent dimensions that describe the larger part of the variety in organization practices. The six dimensions found in their research were (1) process-oriented versus results-oriented: which opposes a concern with means (technical bureaucratic routines) against a concern with goals and outcomes; (2) job-oriented versus employee-oriented: which opposes a concern for the employees job performance against the concern for their well-being; (3) professional versus parochial: opposes the concern where employees derive their identity primarily with their profession against members deriving their identity from the organization which they work for; (4) open systems versus closed systems: this dimension refers to the common style of internal and external communication and the ease with which outsiders and newcomers are admitted; (5) tight versus loose control: this dimension deals with the degree of formality and punctuality i.e. the internal structuring within the organization, it partly is a function of the unit’s technology; (6) pragmatic versus normative: this dimension describes the prevailing way (flexible or rigid) of dealing with the environment particularly with customers (Hofstede, 1990).

<table>
<thead>
<tr>
<th>Hofstede’s Six Dimensions of Organizational Culture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process-Oriented</td>
</tr>
<tr>
<td>Job-Oriented</td>
</tr>
<tr>
<td>Professional</td>
</tr>
<tr>
<td>Open System</td>
</tr>
<tr>
<td>Tight Control</td>
</tr>
<tr>
<td>Pragmatic</td>
</tr>
</tbody>
</table>

Table 2.2 – Hofstede’s Six Dimensions of Organizational Culture
Hofstede (2011) came to the conclusion that organizational cultures reside rather in (visible and conscious) practices: the way people perceive what goes on in their organizational environment. The multidimensional model of organizational culture does not support the notion that any position on one of the six dimensions is intrinsically “good” or “bad”, labeling positions on the dimension scale are a matter of strategic choice (Hofstede, 1990).

In their 2000 publication on linking culture to improvement initiatives in organization, Detert et al, succeeded in synthesizing eight cultural dimensions and their relation to a specific improvement initiative (Total Quality Management – TQM). Their organizational cultural framework of TQM values and beliefs identifies these cultural dimensions that most related to the change of programs to improve important human and organizational values. The eight dimensions are: (1) the basis of truth and rationality in the organization: Decision making should rely on factual information and the scientific method. Focuses on the degree to which employees believe something is real or not real and how truth is discovered; (2) The nature of time and time horizon: The concept of time in an organization has baring in terms of whether the organization adopt long term planning, strategic planning and goal setting, or focus and reacting on a short time horizon; (3) Motivation: Employees are intrinsically motivated to do quality work if the system supports their efforts. Management should identify whether manipulating others’ motivation can change effort or output of employee; (4) Stability versus change/innovation/personal growth: Organizations that are risk-taking always stay innovative with a push for constant, continues improvement. Risk-averse organizations tend to be less innovative, with little push for change. ; (5) Orientation to work, task, and co-workers: The main important issues here is the responsibility employees feel for their position and how they are educated in terms of their roles and responsibility; (6) Isolation versus collaboration/cooperation: Cooperation and collaboration (internal and external) are necessary for a successful organization. In some organizations, collaboration is often viewed as a violation of autonomy; (7) Control, coordination, and responsibility: A shared vision and shared goals are necessary for organizational success. All employees should be involved in decision making and in supporting the shared vision; (8) Orientation and focus-internal and/or external: An organization may decide to have internal orientation focusing on people and processes within organization or emphasize on external orientation focusing on external competitive environment, or have combination of both, Lim et al. (2009)

<table>
<thead>
<tr>
<th>Detert et al. (2000) - Eight Dimensions of Organizational Culture</th>
</tr>
</thead>
<tbody>
<tr>
<td>The basis of truth and rationality in the organization</td>
</tr>
<tr>
<td>The nature of time and time horizon</td>
</tr>
<tr>
<td>Motivation</td>
</tr>
<tr>
<td>Stability change/innovation/personal growth</td>
</tr>
<tr>
<td>Orientation to work, task, and co-workers</td>
</tr>
<tr>
<td>Isolation collaboration/cooperation</td>
</tr>
<tr>
<td>Control, coordination, and responsibility</td>
</tr>
<tr>
<td>Orientation and focus-internal and/or external.</td>
</tr>
</tbody>
</table>

Table 2.3 – Detert et al.’s Eight Dimensions of Organizational Culture
2.10 Organizational Culture & Employee Behaviour

In his clarification of culture, Schein (2004) reveals that it is both a dynamic phenomenon (we are immersed in, which is constantly being created, enacted and shaped in our interactions) and a set of structures, routines, rules, and norms that guide and constrain behavior.

To further buttress this point, Thomson et al. (2006) stipulates that the relationship between organizational culture and employee behaviour is something that should be considered when implementing security practices. This is because it impacts on how employees behave, places a constraint on their activities and prescribes what they and the organization must do. Robbin (1998, see Lim et al., 2009) from his perspective explains that organizational culture among others, acts as a sense-making and control mechanism to guide and shape the attitudes and behaviours of employees.

Triandis et al. (2002) in his work on “Cultural Influences on Personality” reveals that although personality is shaped by both genetic and environmental influences, the most important of the environmental influences is that of culture. Behaviour they go on to explain is not only a function of both this personality and culture but also varies depending on the interaction between the personality and the situation in which one finds him/her self. A number of researchers including Dhillon et al. (2000), Schlarman (2001) and Thomson et al. (2006) have similarly emphasized the importance of understanding organizational culture, such as beliefs, values and assumptions when working with policies and users’ actions, (Karlsson et al, 2008).

Maccoby (2000, see Triandis et al, 2002) also explain that ecology among other factors shares culture which in turn shapes that socialization patterns and which shape some of the variances of personality

According to Pascale (1985, see Hofstede, 1990), organizational practices (i.e. culture) are learned through socialization at the workplace. For most newcomers to an organization, much of the socialization process is therefore embedded in the organization’s normal working routines. It is not necessary for newcomers to attend special training or indoctrination sessions to learn important cultural assumptions; these become quite evident through the daily behavior, (Schein, 2004). Security culture therefore supports all activities in such a way that, information security becomes a natural aspect in daily activities of every employee, Schlienger and Teufel (2002),

The environment that has the most influence on the employees’ beliefs and attitudes is that of culture within the organization, therefore the power to change the culture of an organization lies largely with senior management ,Drennan (1992, see Thomson et al. 2006)

2.11 Organizational Culture, Information Technology & Performance

Culture is abstract, yet its influence in social and organizational situations is powerful, Schein (2004). It is essential because, it’s tacit and often unconscious influence determines individual and collective behaviour, perception and thought patterns as well as values. Organizational culture in particular is indispensable because, its constituents determine strategy, goals, and modes of operating Schein (2006).

Culture is a property of a group, because whenever a group has enough common experience, it begins to form. One finds culture at the level of small teams, families and work groups. It also arises at the level of departments, functional groups, and other organizational units that have a common occupational core and common experience. It is found at every hierarchical level but it exists at the level of the whole organization if there is sufficient shared history Schein (2006).
The past decade has seen considerable increase in the impact of culture on the development and use of information and communication technology and there is the clear need for global organizations to understand the relationship between organizational culture, information technology and information security, Yeganeh (2008). Yeganeh (2008) goes on to say that notwithstanding the fact that technology may be free of culture; some technologies such as IT may not be culture-free because they are affected by human behaviour.

IT is an important component of the organizational decision making and most managers rely on it to aid their decisions, Yeganeh (2008). In his research Yeganeh (2008) concludes that when culture is in agreement with IT it; lays down the patterns for the usage of information, creates cohesion among organizational members and allows the creation of social controls among others. Schein (2009) also similarly argues that if we want to make organizations more efficient and effective, then we must understand the role that culture plays in organizational life.

Kim (2004) in his view relates organizational performance to “the degree of success in realizing an administrative or operational function in relation to institutional mission”. He reveals that sometimes the initial founders of a firm (or management teams) consciously decide to improve the performance of their firms using the power that resides in developing and managing a unique corporate culture, citing examples of G.E, McDonalds, Disney and Microsoft. Sorensen (2001) also stresses that having widely shared and strongly held norms and values lead to performance benefits such as: enhanced coordination and control within the organization, increased employee effort, and improved goal alignment between the organization and its employees.
3 Framework of Ideas

To carry out our investigation, we researched into a number of frameworks that will assist us in developing an appropriate concept to guide us in answering our research question. In pursuing the numerous frameworks, theories, models and principles, we were not looking to identify just any kind of culture that exist in the organization but specific cultural traits which will have an influence on the successful implementation of information security policies. It must be explained here that the term “implementation” is used to denote the realization of the policy’s requirements, which is to get employees to think act and behave in a way that impacts on the protection of the organization’s information assets.

3.1 Information Security Policy Process Model

The first of this frameworks was one that will aid us establish the overall relationship between information security policy implementation and organizational culture. For this we chanced on the Information Security Policy Process Model developed by Knapp KJ et al (2009). In their work on developing an organization process model for information security policy Knapp et al.(2009) gathered data by asking respondents (CISSP professionals) to provide information on the top five information security policy issues facing their organization (Knapp et al., 2009). They then used it to depict the policy model as a repeatable organizational process. The repeatable process then took into consideration a number of external and internal factors to develop the final model as depicted below

Our interest in the model is that it establishes the overall relationship between organizational culture and the information security policy which is the focus of our study. In explaining Knapp et al. (2009) reveal that it is the organizational culture that will significantly determine the overall employee attitude towards security. They cite as an example the work of security staff will be untenable if employees develop hostility towards a policy that they find unreasonable.
3.2 The Organizational Culture Framework

Detert et al. (2000), in their search for a framework to link culture to improvement initiatives in organizations, also came up with a framework to describe and measure culture in organizations. They arrived at this by synthesizing and dimensionalizing OC frameworks (including that developed by Hofstede et al. (1990): Measuring Organizational Culture, Schein (1992): Organizational Culture & Leadership and Cameron & Freeman (1991): Competing Values etc.) developed by previously researchers in the field of organizational culture and identified which of these dimensions most related to the change of programs to improve important human and organizational effects, Lim et al. (2009). They then linked these to values and beliefs that formed the “cultural backbone” of successful total quality Management (TQM) adoption, Lim et al. (2009). They then came out with eight overarching cultural dimensions which we will also utilize in our research to develop and justify the foundations of our organizational cultural goals for information security policy implementation.

*See Table 2.3 for a diagrammatical representation of the eight dimensions organizational culture

The full explanation and meaning of the framework and its dimensions as taken from Detert et al.’s (2000): A Framework for Linking Culture and Improvement Initiatives in Organizations is discussed in Section 2.7

3.3 Framework of the Relationship between Organizational Culture (OC) and Information Security Culture (ISC)

Lim et al. (2009) base their research on Detert et al.’s (2000) Organizational Cultural framework among others to explore the influence employee actions and behaviours have in relation to information security practices. They gathered from previous literature that Information Security Culture (ISC) was still not be embedded in organizational Culture (OC) because of the following challenges: ISC was not an integral part of OC, insufficient budget for security activities, locus of responsibility, organizational motivation towards implementing security measures and different perceptions towards security risk, Lim et al. (2009). They accordingly developed a conceptual framework that could be used to assist organizations to determine the extent to which (ISC) is embedded in OC using cultural views by Fitzgerald’s (2007) and other researchers to establish the nature of the relationships. Three types of relationships were developed in their resulting framework to measure whether ISC was embedded in OC, a subculture of OC or is separated from OC.

Our research and final theoretical model is primarily based on the work carried out by Lim et al, (2009) as we used a majority of the requirements they identified under OC and ISC in addition to that from other previous literature to arrive at our set of organizational cultural characteristics necessary for determining information security policy success. Their framework showing the nature and type of relationship between OC and ISC is shown below
<table>
<thead>
<tr>
<th>Nature of Relationship</th>
<th>Organizational Culture (OC)</th>
<th>Employees Beliefs, Actions and Behaviours (ISC)</th>
<th>Probable Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type 3 relationship:</strong></td>
<td>Management Involvement: Management bring security matters and strategy into board meeting Updates are made on a periodic basis to the company board of directors</td>
<td>Responsibility: Always adhere to the security procedures and guides.</td>
<td>Risk Vulnerability: Low</td>
</tr>
<tr>
<td>Where ISC is embedded into OC. (Von Solms, 2000; Schlienger, T. &amp; Teufel, 2002; Thomson et al., 2006)</td>
<td>Locus of Responsibility: Management involves every member of the organization</td>
<td>Participation: Employees undergo periodic security training, awareness programme</td>
<td>Awareness: Employees are highly aware and concerned about security matters in organization.</td>
</tr>
<tr>
<td>High (Fitzgerald, 2007)</td>
<td>Information Security Policy: Created in holistic manners. In addition, there are regular updates on security policy.</td>
<td>Commitment: Employees feel responsible and ownership of information.</td>
<td>Responsibility: Security is every employee’s business.</td>
</tr>
<tr>
<td></td>
<td>Budget Practice: Management allocates budget for security activities annually.</td>
<td>Awareness/Know how: Know-how and who to deal with when facing security problems</td>
<td>Investment for Security Practices: High cost in implementing security activities.</td>
</tr>
<tr>
<td><strong>Type 2 relationship:</strong></td>
<td>Management Involvement: Management typically delegates understanding of information security matters to CIO.</td>
<td>Responsibility: Adhere to security matters as a requirement of management</td>
<td>Risk Vulnerability: Medium</td>
</tr>
<tr>
<td>where ISC is a subculture of OC (Dutta &amp; McCrohan, 2002; Ramachandran et al., 2008)</td>
<td>Locus of Responsibility: Management starts to empower security</td>
<td>Participation: Employees are involved in security matters in own dept. Less Departmental coordination.</td>
<td>Awareness: Employees are aware of security matters within their own dept.</td>
</tr>
<tr>
<td>Moderate (Fitzgerald, 2007)</td>
<td></td>
<td></td>
<td>Responsibility: Employees are responsible for security within their own dept.</td>
</tr>
<tr>
<td><strong>Type 1 relationship:</strong></td>
<td><strong>Management Involvement:</strong></td>
<td><strong>Responsibility:</strong></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------</td>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td>where ISC is a separated from OC (Chia et al., 2002; Knapp, Marshall, Rainer et al., 2004; Shedden et al., 2006)</td>
<td>Management intuitively knows that information security is important, but assigns the same level of importance as ensuring that computer is up</td>
<td>Do not care and not responsible towards security matters</td>
<td></td>
</tr>
<tr>
<td><strong>Locus of Responsibility:</strong></td>
<td>Management assigns all security responsibility to IT department.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Information Security Policy:</strong></td>
<td>Created by copying without the means to enforce them. Usually issued by a memo.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Education/Training:</strong></td>
<td>Low awareness. Management does not</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **Commitment:** | Responsible and committed in security matters for own dept. | |
| **Motivation:** | Employees are motivated in security matters in own dept. | |
| **Awareness/know-how:** | Know-how and how to deal with when facing security problems within own department. | |

| **Practices:** | Security is employee’s routine activities within their own dept. | |
| **Investment for Security Activities:** | Medium cost in implementing security activities | |
Table 3.1 – Framework of the relationship between Organizational Culture and Information Security Culture. Lim et al (2009)

<table>
<thead>
<tr>
<th>Emphasize on security training.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Budget Practice:</strong></td>
</tr>
<tr>
<td>usually part of a budget for IT support</td>
</tr>
</tbody>
</table>

3.4 Schein’s Three Levels of Culture

The essence of Schein’s three levels of culture is to enable us decipher exactly what culture is, as it pertains to an organization’s context. This is especially important because culture is broad, complex and not easy to quantify, a reason why Schein (2004) describes the deepest essence of culture as less tangible and less visible. To make it tangible Schein (2004) breaks it down into this identifiable constructs, where artifacts are the visible structures and processes that exist in an organization. The philosophies, ideologies and strategies that are espoused by an organization which are usually only rational aspirations rather than the actual values are what he classifies into the second level. The third level which he explains as deep seated, invincible, unconscious are what forms the foundations of all culture and he calls this assumptions. Based on these classification of culture, we can therefore move confidently into an organization, having the appropriate theoretical spectacles (framework), which will aid us define and profile their culture.

*See figure 2.3 for a diagrammatical representation.*

As mentioned above, culture is broad and disparate and there is a need to identify and focus on the particular organizational culture that is relevant to our study. To ensure that the study and analysis of the organization’s culture is done in a more targeted manner, we will require the appropriate “lens” specifications to enable us focus on only what is required and not all that lies in our view. We must therefore find or develop the lens with the appropriate specifications so we can focus only on organizational culture that is relevant to information security and information security policy implementation to be exact.
3.5 Bringing the Theoretical Ideas Together

It is necessary to put the theories discussed together to determine the direction of the study and set a basis for a theoretical proposition. The relationship between information security policy implementation and organizational culture, is deduced from work by Knapp et al. (2009) in their research on the Information security Policy process model which establishes organizational culture as an internal influence to the information security policy process. It is this organizational culture they reveal, that significantly determines the overall attitude of employees towards security; which has information security policy as its foundation.
Organizational culture however is broad and there is a need to zero-in on the relevant organizational cultural traits or characteristics that inure to the benefit of information security policy success. To do this, we rely on a number of frameworks including the work done by Lim et al (2009) in their “Exploring the Relationship between organizational culture and information security culture” to identify characteristics that ensure “information-protecting” behaviour on the part of the employees. We also rely directly on a number of the dimensions of Detert et al (2000) in their Organizational Cultural Framework, to identify the cultural characteristics that are relevant to securing the information assets of an organization.

These Information-Protecting characteristics of the organization’s culture is what will ensure that the goals of information security policy (To get employees to behave, think and act in a manner that protects the organization’s information asset) is achieved and it is called Information Security culture.

It is therefore relevant that the culture that will lead to successful security policy implementation is one that is “information- protective” and this is why information security culture is explored as the phenomena to ensure appropriate employee behaviour.

Schein’s (2004) three levels of culture enables us to explore culture as an identifiable entity so we can examine it in the different forms that it exists. As explained earlier, culture exists at three different levels in the forms or Artifacts, Espoused values and Underlining Assumptions. This theory particularly aids us in the data collection stage as it ensures that the different perspectives of the same cultural data is holistically captured in all its forms, serving as a sort of theory triangulation.

3.6 Theoretical Proposition

From our study and analysis of the various frameworks, theories and models of organizational culture, information security policies et al., as detailed in the literature review in prior chapters, we have deduced and are proposing a model of cultural traits that will used as a cultural assessment guide to identify characteristics that an organization should have in order to successfully implement IS policies. This proposal as stated earlier is founded on the belief that, the challenges faced by ISP implementation can be traced to the socio-cultural context of the organization where the policies are being implemented. For an organization to be deemed culturally prepared to follow through and execute ISP successfully, it should have, and portray these characteristics as it exists at the three cultural levels (Artifacts, Espoused values, underlying assumptions). Because (of course) these cultural traits will also have to be “lived” in the case organization and not just espoused or displayed, data collection will have to take place at a number of levels to confirm and establish the existence of these traits. It must be noted however that the model (i.e. the characteristics) are not qualities of the organization as an entity alone. It also relates to the behavioural of the employees in the organization, not as their individual personalities (which may be inherited) but as qualities which they have acquired whilst immersed in the context of the organization. This is corroborated in Hofstede’s (1993) definition of culture as a collective programming of the mind which distinguishes one group from another. It is also supported by his (Hofstede) three levels of uniqueness in human mental programming where he states that personality is both inherited and learned but culture is specific to a group. The content and result of the collective programming can be elicited from the members of the group by way of their behaviour. That is to say, if they (members of the group) have been programmed mentally in a particular way, it is likely to show up in their behaviours or actions, particularly when operating in the context of where they are programmed.

We have also followed a path similar to that pursued by Detert et al. (2000) to analyse and synthesis the frameworks we have come across in our study of organizational culture, Information security

33 |
culture and policy implementation to develop this framework. This framework is developed from ten ‘mutually’ exclusive cultural characteristics that we have found, when present in an organization will naturally “manage” and steer employee behaviour into appropriately performing the requirements of an information security policy. The ten characteristics are (1) Management Style, (2) Trust & Responsibility, (3) Bureaucracy & Dependencies, (4) Motivation, (5) Budget and Funding, (6) Awareness, Education & Training, (7) Participation, (8) Commitment, (9) Communication, (10) Supervision, Co-ordination & Control. These characteristics have been found to stimulate the behaviour and actions of employees, leading to a culture that influences the successful implementation of IS policy.

3.6.1 Management Style

According to Desson & Clouthier (2010), the focus of management and their style of operation are pertinent to achieving success. They mention that this is evident in their priorities, whether they are consultative and staff perception about management’s ability to “walk the talk”. It is also general knowledge that security is every body’s business. In light of the consultation, March (1991) advises organizations to develop the willingness to learn from their members to better understand and cope with changes in environmental conditions, a phenomena they term “cultural exploitation”. Fung & Jordan (2002) exclaim that management has the tendency not to initiate information security measures because they generally feel it is the responsibility of the IT department.

From Lim et al.’s (2009) perspective, this relates to management bring up security matters and strategies to the attention of the board and their decision to get involved in security discussions and implementations to foster their understanding and appreciation of security. In this regard, if management sets the implementation of ISP’s as a priority and endeavors to consult on issues of implementation as well as getting involved, just as they have advised, one is likely to see results with ISP implementation.

Ruighaver et al. (2007) also discuss how tight the decision making process of an organization is as this influence the tolerance level of individual initiatives. This also relates to who has decision rights with regards to security also. Lim et al. (2009) found among other that there were different perceptions held of security risk in the organization. Management therefore needs to establish this by establishing security authority and issuing a singular position of risk from the top. Hone & Eloff (2002) explain that the behaviour and attitudes of employees towards information security will be more in line with secure behaviour if top management demonstrates concern, therefore it is suggested that the tone of security is set by the attitudes of those at the top of the organization.

From the ISP implementation perspective this can be tied down to management’s involvement, understanding and appreciation of the ISP implementation process. It also pertains to whether they have appropriately prioritized the policy implementation process which is broadly based on whether it has been discussion with the board to ensure that the importance of the process is appreciated from the very top. Schein, 1992, see Lim et al, 2009) also reveal that organizational culture is formed by the behaviour of the dominant organization’s members such as top management and this is reflected in their style of management.

3.6.2 Trust & Responsibility

Dhillon and Backhouse (2000) in their definition of the RITE principle, reveal that is it pertinent for employees to understand their roles and responsibilities in this changing world of disappearing vertical management structures. They go on to explain the employees must therefore be able to develop their own work practices on the basis of understanding the responsibilities especially when met with an
unusual or unexpected situation. Also in their explanation of trust, they confirm that the lessening of external supervision requires that employees be trusted to abide by organizational codes and norms.

In their discussion of the implementation plan for security, Whitman and Mattord (2009) talk of how tasks in the implementation process should be appropriately assigned to relevant members of the team. This they say should be preceded by a clear and unambiguous description of the task to be accomplished. Ruighaver et al. (2007) argue that the staff responsible for security implementations feel a high sense of ownership but that this ownership is influenced by the level of social participation that staff have in security. Maynard et al. (2002) however insist that the overall responsibility for security should be given to an empowered security team.

3.6.3 Bureaucracy & Dependencies

Hofstede (2011) discuss this attribute in relation to their process-oriented Vrs results-oriented dimension. He reveals that the process-oriented cultures are dominated by technical and bureaucratic routines, whilst results-oriented only focuses on goals on outcomes. It also relates to power structures that exist in the organization to inhibit the smooth process of implementation. Whitman and Mattord (2009) advice that planners of IS implementation should note wherever possible the dependency of other tasks on the tasks at hand. They advise taking note of precursors and successive tasks to that which is at hand to ensure that they are taken care of accordingly.

3.6.4 Motivation

Ruighaver et al. (2007) in interpreting Detert et al.’s (2000) framework reveal that motivation relates to processes that are in place ensure that employees are well motivated in relation to security. This they say also includes tangible rewards (i.e. money) especially with the expectation of increased or slightly modified performance standards and behaviour of employees (Pierce et al., 2003). Ruighaver et al. (2007) goes on further to reveal that this also includes, the organization not contradicting their own values in trying to achieve security goals, which makes employees reluctant in supporting security initiatives. This can also lead to little co-ordination of security. They go on to explain that in the case where some organizations delegate security responsibilities from management to each and every employee, it leads to peer-pressure to abide with policies and procedures. The conclusion is that, motivation is ensured through the encouragement of broader mix of horizontal and vertical social participation. Ruighaver et al. (2007) further reveal that the motivation of staff is lowered if they feel that their suggestion on security improvement are not considered, the situation can be easily solved if there is a positive response by management to some of the suggestions made. Lim et al (2009) reveal that employees are also motivated to do quality of work if the system supports their efforts.

3.6.5 Budget and Funding

According to Al-Awadi et al. (2007) all the interviews they carried out during their research had the experts define budget as an important aspect of implementing information security in the organization. They further found out that without enough budget, organizations won’t be equipped with the necessary resources (software, hardware, consultants) to ensure information security. Whitman and Mattord (2009) similarly reveal that any project should be accompanied by a clear financial estimate of all expenditures (both capital and nominal). This they say relates to whether the organization has appropriate budgeted funds for the implementation of a security policy. All policies should also ideally come with some amount of financial commitment to ensure that the implementation is successfully
carried out. From Anderson & Moore’s (2006) perspective, budget generally depends on the manner in which individuals’ investments translate to outcomes, but the impact of the investment also depends on the decision of the investors and others. Al-Awadi et al. (2007) advice that information security expenses should be analyzed in cost-benefit manner and it should not be just investment in expensive software or hardware.

Al-Awadi et al. (2007) conclude that resources in organizations are the foundation requirement to enforce and monitor the implementation of information security for which Dinnie (1999) says a lack will lead to under-investment in appropriate controls.

### 3.6.6 Awareness, Education and Training

According to Knapp et al. (2009), the importance of security awareness training and education cannot be overstated and that one of the basic steps in coping with information security risk is the establishment of an awareness training program. This position is supported by (ISO/IEC, 2005) who urge organizations to train employees about the security threats and to encourage employees to support organizational policy in the course of their daily work. Whitman & Mattord (2009) however states it rather more emphatically when they reveal that paramount in the process of implementing information security policy is the need to keep the policies fresh in the minds of employees, although they recognize it as one of the greatest challenges in implementing information security in general. This emphatic position is similarly expressed by Al-Awadi et al. (2007) who stress that information security would need a continuous and ongoing awareness and training programme for employees to deal with the ever-changing security arena. Dhillon (1999) also argues that, organizations need an ongoing education and training programs in order to achieve the expected outcome from the implementation of an information security policy.

From another perspective, Lim et al. (2009) see awareness and education to include how management periodically update and inform the board of the company with issues related to security. They believe that this characteristic deals with employee’s knowledge of how to deal with security situations they are confronted with. They also discuss this attribute in terms of the strictness with which management attaches to employees attending awareness programs and supports for training programs related to security. Verton, 2000 & Shipley, 2000 (see Maynard et al, 2002) however choose to place the education on security at the upper levels. They argue that awareness should be initiated from the highest levels in the organization and this will drive the proper education of all employees. This initiation however should be done in collaboration with the security team.

Knapp et al. (2009) further reveals that awareness is often viewed as a tool to address and improve on the overall behavior and conduct of employees. They also state that awareness training should not stop at just understanding the policy but also the rationale behind the policy and the risks of non-compliance. Al-Awadi et al. (2007) more instructively recommends that a training and awareness program should be carried out for all employees at all levels, whilst taking the employees job type and environment into consideration. They for example suggest that, awareness training for managers vary from other employees in the IT department and so forth.

Vroon & von Solms (2004) conclude that employee violations of IS security policies is largely due to negligence and/or ignorance.
3.6.7 Participation & Coopération

Lim et al. (2009) relates this to how employees get involved in security matters in their work units and their level of participation in awareness programs or other periodic security trainings alike. According to O'Reilly & Chatman (1996), when employees participate in group activities or decision making such as security goal setting, it makes them feel important to the group and their efforts are increased. Flechais & Sasse (2009) argue that the key element of participative approaches to (design, development and implementation of systems) revolves around representing the relevant viewpoints of different parties in such a manner as to achieve a consensus. This position is similarly posited by Clark-Dickson (2001, see Maynard et al, 2002) who mention that security policies should be created collaboratively with the input from various employee groups in the organization in order to make it comprehensive and acceptable.

3.6.8 Commitment

Pareek (2004) defines organizational commitment as a person’s feeling with regard to continuing his or her association with the organization, acceptance of the values and goals of the organization, and willingness to help the organization achieve such goals and values. Deducing from Luthans (1995) perspective, this is an attitude where the employee has a strong willingness to exert high levels of effort on behalf of the organization. They also reveal that it usually comes with some expectation in return such as a work environment that provides the necessary resources and which fosters growth & development among others. This characteristic according to Hellriegel (2001) however goes beyond loyalty to include an active contribution to accomplishing organizational goals. He further explains that it represents a broader work attitude than job satisfaction because it applies to the entire organization rather than just to the job. He also reveals that it is more stable than satisfaction because day-to-day events are less likely to change it. From Lim et al.’s (2009) understanding and in relation to information security, it involves the employees feeling and ownership of information. Pahnila et al. (2007) also discuss this attribute in relation to compliance, i.e. the attitude, intension and actual compliance with IS policies. They go on to reveal that this requirement can be achieved through social pressure (normative belief) towards IS policy from top management, supervisors, peers and security staff.

3.6.9 Communication

In their discussion and encouragement of social participation along horizontal and vertical lines, Ruighaver et al. (2007) reveal that there are numerous instances where employees at the same level within different areas come across the same security issue and may not know that it has been covered by other in the same organization. In this same manner there is likely to be a situation and information common to one group of people may not be known by others within the same organization. This calls for a system where information is shared among all relevant members of the organization, in this case all those involved in the ISP implementation. Hofstede (2011) also discusses this attribute in his Open System Vrs Closed system dimensions where he talks of the common style of internal and external communication, particularly with regards to the ease or otherwise with which outsiders and newcomers are admitted. With regards to this, Kolkowska (2003) reveals that curiosity is minimized if communication is open. Flechais and Sasse(2009) better analogizes the need for communication when they cite an example of where two different employee groups or individuals assume that an issue is the responsibilities of another (diffusion of responsibility) which generates problems. They therefore go to posit that the process of socio-technical design is fundamentally an issue of communication between different parties in a system, and without effective communication, relevant design information will be
impossible. They conclude that successful communication will therefore be achieved if stakeholders share knowledge and points of view will minimal confusion and bias.

3.6.10 Supervision, Co-ordination & Control

Whitman and Mattord (2009) in their discussion of security program implementation mention that some organizations designate a champion from the general community of interest or alternatively select a senior IT manager to lead the security implementation. This role may usually be the same as a policy administrator who is responsible for the creation, revision, distribution and storage of the policy. This individual is also the one who notifies all affected members when policy is for example modified. This function can also come under the cultural trait of trust and responsibility where, it must be required that one person is availed to man this position. This is in alignment with Hinde’s (1998, see Maynard et al., 2002) assertion that the tone for security needs to be set from the top of the organization. In discussing the organizational culture framework of Detert et al. (200), Ruighaver et al. (2007) relates control to the governance of security where an organization with centralized decision tends to have a tight control whilst that with flexible decentralized decision making tends to have loose control. Hofstede et al. (1990) in his six dimension of organizational culture also similarly discusses this concept from the perspective of the degree of formality and punctuality within the organization. Ruighaver et al. (2007) further explain that because security culture is not independent, tight security culture in the context of a loosely controlled organization is also like not to work. This they say has been evident in the case study of organizations where organizations with high security requirements have tight control over processes and policy, with manifestations of formality. Monitoring processes also ensure that implementation is going on according to plan.
4 Research Approach and Design

4.1 The Research Approach

The research domain of investigating the influence of organizational culture on information security (policy) implementation, to solve the employee behaviour problem and achieve success is a relatively new area with limited previous research (Lim et al, 2009). We therefore among others, hope to use this study to add to the limited research and open up a platform to guide more researchers in this direction. A definite and established theoretical framework does not exist to assist with answering the research question hence there is a need to explore pertinent literature and develop an appropriate conceptual framework that will guide and enable us meet the objectives of this study. The research journey follows that of an exploratory path, which as suggested by Yin (2009) is the approach to be used if existing knowledge or theory is poor, with no relationship established; which is what we intend to find out. He explains further that the focus of the study should be on what is being explored, the purpose of the exploration and the criteria for judging the success of the study. We are threading a similar path where theory on the influence of organizational culture on information security implementation is weak; we will therefore pursue the study with a focus on organizational culture, and through literature review develop an initial proposition.

4.2 Case Study as a Research method

Case studies according to Yin (2004) are particularly suited for answering “How” and “Why” questions. He explains that a case study is most suited for investigating contemporary phenomena in its in-depth real life context especially where the bounds between phenomena and context are not clearly evident. Stake (1995) also suggests that a case study is useful when “opportunity to learn is of primary concern”. This suggestion is similar to that of Leedy & Ormrod (2005) who reveal that a case study may especially be suitable for learning about a little known or poorly understood situation and that it is useful for generating or providing preliminary support for a hypothesis. To differentiate case study as a method from experiments, Yin (2004) reveals that the difference lies in the extent of control that an investigator has over the behavioural events. The contrast between it and the historical method is the way in which it focuses on contemporary events which the historical method does not. By the criteria of “focus on contemporary events” and “control over behavioural events; it therefore shares similarities with a survey method, however the survey approach focuses more on the prevalence of a phenomenon or the prediction of an outcome whereas the case study is more explanatory in nature, Yin (2009). In that the implementation of information security policies (the phenomena) is bound and tied to an organizational context, this investigative approach is clearly suited for our research agenda. Our research agenda which is clearly in the domain of the how (i.e. how organization culture can influence security policies implementation) is therefore well suited for case study.

Yin (2009) distinguishes between three types of case studies, descriptive: which aims to present a complete description of a phenomenon; exploratory: which attempts to define a question or examine the feasibility of an in-depth study; and explanatory, which attempts to offer a cause-and-effect relationship. Stake (1995) differentiates between an intrinsic case study, in which the researcher is interested in the case per se, and an instrumental case study through which we aim to learn about a broader phenomenon and not just the specific case.

From a layman’s point of view, we basically want to find out whether the culture that exists in an organization is “healthy” or conducive enough to facilitate achieving success with information security policies. This therefore warrants that we walk an exploratory path to examine the feasibility of organizational culture being used to achieve success with information security policies.
4.3 The Case Study Design

According to Yin (2004), there are five components to the design of a case study that are particularly important, these are (1) A study’s questions; (2) its propositions, if any, (3) its unit of analysis, (4) the logic linking the data to the propositions and , (5) the criteria for interpreting the findings. In this research the Study question is: What is the influence of organizational culture on the successful implementation of information security policies? ; The Proposition, which we have deduced from literature review is: There are ten cultural characteristics that an organization must subscribe to in order to achieve success with information security policy implementation; The unit of Analysis: Going by explanations given by Baxter & Jack (2008), this case has two possible units of analysis, that is the Policy Implementation process and Organizational Culture. The focus and what is of interest to be analysed in this case however is the culture of the organization, this therefore makes the culture of the organization the unit of analysis; The logic linking data and the propositions : will involve pattern matching logic, this basically involves matching the culture identified in the case organization against the model of cultural traits that was developed; The criteria for interpreting the findings is : If the ten cultural characteristics that have been deduced from extant literature are identified as integral to the organization, then the organization will achieve success with information security policy implementation. Per Yin’s (2009) explanation we will also including the collect of alternate cultural traits (different from the ten deduced) when identified. These cultural traits will then serve as possible rival explanations for achieving success with ISP in a further research.

This study being exploratory in nature is not meant to be the whole story but an initial step towards later research in this direction. According to Yin (2009), with exploratory inquiries all kinds of research methods can be used but case studies seem particularly suited when the goal is to develop pertinent. Huws & Dahlmann (2007) Explain that case studies are carried out in order to investigate newly identified phenomena and develop some initial concepts and hypothesis. These results can then be analyzed in order to produce indicators which can be investigated further.

4.4 Case Organization Selection

In selecting UNICEF GHANA as the case organization, the biases of national culture (as explained by Hofstede’s (2011) Dimensions of National Culture) are removed in examining the organizational culture and affirming the theoretical proposition against data collected there. The choice of UNICEF GHANA in some respects represents both a typical as well as a revelatory case. It is revelatory because, we have a situation where one of the researchers has already been immersed in the culture of the organization over the years (as an employee) and this gives us insight and access that may not be readily available or possible for an outside researcher. It is may also be regarded as a typical representation because it characterizes a regular organization that has its own organizational cultural environment and Information security policy (ISP) in place with concerns to achieving greater success with the policy.
4.5 The Research Journey

4.5.1 Literature review

In our bid to find answers to the research question posed, we went beyond the immediate bounds of information security into other branches of knowledge include psychology, sociology and the specific areas of culture & Organizational Culture.

We began the process by reviewing relevant previous research and articles on culture and how it could be identify and capture as a tangible artifact or data that could be analysed and conclusions drawn. Drawing on the substance of previous research, we were initially fixated on research mainly by Shalom Schwartz, who in his Schwartz model/Schwartz values theory, postulated that cultural dimensions of values reflect the basic issues or problems that societies must confront in order to regulate human activity (Schwartz, 1999). Further study of his research and other material revealed that there was a grandfather theory that Schwartz had used as the basis of his research and this was Hofstede’s model of national culture. Hofstede developed his theory of work values to make sense of data gathered for purposes of management by IBM, Schwartz (2006). The Hofstede’s model gave a lot of impetus to the research since our initial determination was to focus on the Ghanaian socio-cultural context. In re-examining the study objectives and upon further review of previous research material, we found it pertinent to delimit the scope of the cultural influence on security policy implementation to the organization (whilst losing the Ghanaian boundary), since it was in this context that the relevancy of security policy implementation was directly played and lived. Hofstede’s dimension of organizational culture (which opposed 12 organizational characteristics [to create six dimensions] against each other, Hofstede (2011)), his onion diagram (which shows manifestations of culture at different levels of depth, Hofstede (1993)) and Edgar Schein’s three levels of culture (which explains that culture exist at deeper levels founded on underlying assumptions) were the foundation on which the study was investigated from the cultural front. From the Information security policy (ISP) perspective, we used the Information Security policy Process Model of Knapp et al (2009) to tackle the research question. This model establishes a relationship between the overall policy processes (include implementation) and external and internal influences including organizational culture: which the focus of this study. Notwithstanding the fact that this model is not able to profoundly explain (because empirical data is based only on responses to questions posed to CISSP professionals) how organizational culture influences the security policy implementation process, it serves as the first step in the development of a conceptual model to guide the investigation. We then learnt of a number of cultural frameworks including Hofstede’s (2011) six dimensions of organizational culture, Schein’s(2004) three levels of culture, Detert’s(2000) Organizational Culture framework which details his eight dimensions of organizational culture. The defining model that largely shaped our work was Lim et al’s (2009), exploration of the relationship between organizational culture (OC) and information security culture (ISC). The essence of their research was a revelation (through a review of extant literature) of the level of embeddedness of information security culture in organizational culture and a detailing of the constituent characteristics of OC and ISC.

4.5.2 The Research Process

Whilst pursuing this research, collecting & reviewing previous research, we inevitably had to review both the research question and the embedded research questions (in order to suite the objectives that we had in mind. These embedded questions were premised on our initial assumption of hoping to identify certain (uncomfortable) conditions in the organizational setting that were as a result of a lack of some organizational cultural traits.

We initially formulated this sequence of embedded research questions
What organizational conditions are required for the successful implementation of information security policies?

What organizational culture create the necessary conditions that are required for the successful security policy implementation

Through further research however we found out that these conditions we were seeking out were dynamic formations, different from culture and described as organization climate (Yahyagil, 2004). The organizational climate may be as a result of an event or situation in the organization and as explained by Wallace et al (1999), there is a close and sometimes ambiguous relationship between organizational culture and climate which has often been overlooked. The organizational climate represents employees shared perceptions of the organization whereas culture is a result of shared assumptions (Patterson et al, 2005). Schneider (2000) better defines it as the description of things that happen to employees in an organization and it is more behaviour-oriented. He explains further that organizational culture comes to light when employees are asked why certain patterns exist. Capturing data on these climatic conditions may also be difficult to decipher it possible at all; we therefore transitioned the embedded questions to what we currently have stated.

In defining the research question we were at a point where the research question was: What is the relationship between information security and Organizational culture. We were initially hoping to quickly identify a suitable theoretical framework that establishes the relationship between our research variables then use this to gather empirical data using the case organization. The literature review turned out to be a real adventure as we came by snippets of theories, models and frameworks which we had to bring together to form the framework we had initially hoped to find. The information collected from that will support our study.

After reviewing much data and collecting so much available information on some of the cultures that were oriented towards a secure organization, it made no sense to try and re-invent the wheel by gathering empirical data from a case organization. This was because we were likely to come up with the same set of cultural traits that had already been identified by previous researchers. We therefore though it wise to gather, decipher and distil information from the numerous literature we had reviewed to come up with a set of security-oriented cultural traits that will represent, from our estimation, what an organization should possess to be culturally oriented towards achieve success with ISP implementation. The case study organization and its intended empirical data collection exercise were therefore reduced to serving the purposes of theory testing.
5 Data Collection and Analysis

5.1 Data Collection Strategy

According to Cameron (2004), the key to assessing organizational culture, is to identify aspects of the organization that reflect its key values and assumptions and then give individuals an opportunity to respond to these cues. Because of the complexity of culture, Schein (2004) advocates that one needs to have to spend a long period living in the organization to be able to depict the tacit assumptions in the required level of detail. Because of Schein’s (2004) counsel, one may be tempted to conclude that only an ethnographic study is what is required to complete this research. But as explained by Yin (2009), the difference between the case study and ethnographic study (and grounded theory) is the fact that the case study requires the development of theory (which is what we have done by the development of the ten organizational cultural elements) prior to the conduct of any data collection.

With one of the researchers having spent over four years working in UNICEF Ghana office, it afforded us the unique opportunity to carry out this research against the backdrop that over the years, he has had the opportunity to implicitly experience some of the cultural characteristics particularly the underlying assumptions unique to the organization. This situation may not be readily available to an outside researcher. This situation is corroborated by Yin (2009) who explains that among the various rationales for carrying out a single case study is when the case is revelatory. Yin (2009) defines a revelatory case as one that is previously inaccessible or not readily accessible for scientific observation. In this research, the opportunity to participate in and observe both the phenomena (cultural characteristics endowed with security) and the context (the organization) may not be necessarily unique but the descriptive information alone may be regarded as revelatory.

Our resolve to develop a cultural assessment tool to guide the collection of data is corroborated by Schlienger, T. & Teufel, S. (2003) who admit that no unique toolset and method exists by which to study organizational and therefore security culture. In light of this, they posit two main questions that must be resolved by any researcher pursuing this path. The questions are, “what to analyse: according to the used cultural model” and “How to analyse: for the measurement of observable indicators”. To answering this question, we will use the developed model of ten cultural traits and Schein’s (2004) three levels of culture. It must be noted that the use of our model does not abandon the underlying Schein (2004) model on which ours is based, in that, some (if not all) of the ten cultural traits of our model can only truly be determined and established to exist by measuring culture from different perspectives i.e. at the three different levels. For example to truly establish that the cultural trait of “commitment” exists in an organization, you may need to ask questions that will elicit underlying assumptions and not just arrive at that conclusion when the organization has espoused it, probably because it exists as part of its core organizational values. Schein (2004) also brings to light that in analysing culture, it is important to recognize that artifacts are easy to observe but difficult to decipher. This therefore calls for a triangulation (collecting of data from multiple sources) of data to enrich and validate what is collected. Yin (2009) explains that the triangulation of data is not a mere collection of data from multiple sources regarding different facets of the case; it is when you collect information from multiple sources with the aim of corroborating the same fact or phenomenon.

As stated in the research method of organizations by Schein (2004), the best method to investigate culture would have been the clinical method approach (where data comes voluntarily from subjects because they initiated the process or have something to gain) but the circumstances of our current investigation does not afford us the luxury to indulge this approach. Of course this study has not been
initiated by the organization and also the research we are embarking on unfortunately does not readily offer any “sweets” to organizational members. We are intending it to serve as some form of initial study to bolster further research into how relevant organizational cultural values can improve upon the success with security policy implementation. Schein (2004) also advises that to gain more understanding, we must get involved through participant observation/ethnography but this role also risks making subjects get too directly involved leading to a change of the very phenomena being studied. We would however default to the data collection methods shown in the matrix to enrich the data collected. There are a number of advantages and disadvantages to the data collection methods that have been highlighted above.

5.2 Mode of Enquiry

The mode of information inquiry (during data collection) may not necessarily be carried out in such a manner to elicit only information directly related to information security policy implementation, it must be related to culture that is exhibited and permeated throughout the entire organization. It must also be said that the crux of the research may not necessarily be to fashion a separate (information security) culture different from that of the organization per se, it must be to identify the existence of relevant organizational culture which can be strengthened, oriented and improved to achieve successful information security policy implementation. This is because it may be extremely resource intensive to want to create such a specific separate culture. If this is the case, all business units may come in asking for resources to create and enforce culture that is pertinent only to their cause and this is why the building of the culture (which is endowed with security) has to be approached from a holistic perspective. Also should be

5.3 Background of Case Organization

UNICEF was established on 11 December 1946 by the United Nations to meet the emergency needs of children in post-war Europe and China. Its full name was the United Nations International Children's Emergency Fund. In 1950, its mandate was broadened to address the long-term needs of children and women in developing countries everywhere and became a permanent part of the United Nations system in 1953. The specific mission of UNICEF as mandated by the UN general assembly is to advocate for the protection of children’s rights to help meet their basic needs and expand their opportunities to reach their full potential.

UNICEF’s work is carried out in 191 countries through country programmes and National Committees. There are eight regional offices worldwide, as well as a research centre in Florence, a supply operation in Copenhagen and offices in Tokyo and Brussels. UNICEF headquarters are in New York.

At the UNICEF Ghana Country level the organization is headed by the Country Representative (Rep.) who sees to the overall business of the mandate of UNICEF in the country. The hierarchy is followed by the Deputy Representative (Dep. Rep.) who is the Number two in command but most importantly head the actual UNICEF business called the Country Programme in the Country. He has overall supervision of the sections that represent the various areas of interest that UNICEF supports in the country office, although the various sections have their own heads. This areas are slightly different from country to country and in UNICEF Ghana the sections include Child Protection (Who work directly to save guard the rights of children i.e. child labour), Health and Nutrition (with responsibilities such as advocating exclusive breast feeding and Vaccinations, WASH (acronym for Water Sanitation and Hygiene – who look at sanitation and hygiene practices in communities, schools etc.), ACMA (Advocacy, communication, Monitoring and Analysis : have responsibilities to interacting with the
media on the work done by UNICEF), these section is also responsible for social protection policy for women and Children. Another is the Education Section (working with the government to introduce and improve upon policies that will enhance education i.e. advocating girl child education etc.). As mentioned earlier all these sections are supervised by their section heads. There is also the Operation Section which is headed by the chief of operations and is made up of units found in any regular organization such as Human resources, Finance, Administration, supply (procurement) and ICT.

In UNICEF (global as in Ghana) there are three main categories of staff, namely Management, Professional staff and General Staff (G.S). Management is made usually made up of Country Representative, Deputy Representative, Chief of Operations and the various Head of Sections. The Professional Staff includes the unit heads in operations and all individuals that have particular expertise with responsibilities for specific areas such as Education specialist, Communications Specialist etc. The Third category, GS, includes all other junior level staff i.e. ICT assistants, travel assistants, Admin Assistants and the Drivers.

UNICEF Ghana over the years has achieved a stable information security environment which is manifested in ‘virtually’ nonexistence of information security breaches, high compliance rate, effective monitoring and evaluation of information security guidelines. Its information Security policy implementation is also functioning well. Will policies: mainly developed at the global office in NY, being successfully rolled down and implemented in to the country office.

5.4 Participant Observation

As indicated by Guest et al (2013), participant observation immerses the researcher into the how’s and why’s of human behaviour and attitude within the context of study and this makes discoveries natural. This is similar to the position stated in a publication of sociology.co.uk (2013) that, it provides the opportunity for the researcher to know people/organization by getting involved and really understand what is going on including understanding their motives and behaviour from the viewpoint of those been studied. Notwithstanding the revelation by Schein (2004) that culture goes beyond its manifestations and that it actually exists at three levels moving from the very visible to the very tacit and invisible, the reality is that, to enable capturing of data on culture, there has to be some tangible properties or attributes that must be identified and analyzed to enable researchers a reach a conclusive end. Culture is difficult to capture a reason for which most cultural studies or investigations require participant observations where the researcher has to spend a lot of time to enable him/her observe and record those traits of the culture. In our case the opportunity of having one of the researchers already immersed in the case organization’s environment i.e. culture, gives a powerful opportunity to be able to capture these difficult but relevant data. We tried to observe behaviour from the perspective of the ten cultural characteristics. Because one of us is employed in the environment, he took the opportunity of participation and knowledge of activities in meeting, trainings and informal approaches such also corridor conversations and office retreats to decipher employee and therefore organizational attitude towards these activities. He also observed how employees went about their daily operations such as working in a dependent and procedural manner, or in an independent atypical style. This approach helps with capturing data on the Artifacts, which as explained by Schein (2004) includes what is typically observed in the organization, i.e. organizational structures and processes, rituals and ceremonies and its published list of values. He says it also includes organizational charts and formal description of how the organization works. This approach is also useful for capturing underlying assumptions or behaviour that may have been taken for granted but forms part of the culture. This position is supported by Argyris’s (1976, see Schein 2004) definition of underlying assumptions as “theories-in-use”. The best
conceivable ways to capture these “theories-in-use” is by participant observation. To seek further insight into some of the observed behaviour and actions however, interviews will be the tool to use.

5.5 Document Analysis

Bailey (1994) describes document analysis as the analysis of documents that contain information about the phenomenon under study. Payne and Payne (2004) in their view about document analysis described it as the techniques used to categorise, investigate, interpret and identify the limitations of physical sources, most commonly written documents. Document analysis is a form of qualitative research in which documents are interpreted to give meaning to the research topic and then incorporates coding content into themes (Studentvoice.com, 2013). The analysis of the documents was done using the ten cultural characteristics as the frame.

Starting with documents of the organizations mission, vision and strategy, we decoded organizational objectives that goals that fell into any of the ten cultural categories. These documents include the United Nations Staff Regulations & Rules, the 2001 Standards of Conduct for the International Civil Service, The system wide code of ethics, Financial Disclosure Policy among others.

We then moved onto policy documents standards and guidelines to try and identify any of our ten traits embedded in them. We also went through a number of non-ICT related policies especially those related to administrative security in general. UNICEF being who they are (i.e. an agency of the UN) carries a lot of security burden for which it has formulated these policies including UN Security management system, policy manual. There are also a couple of standards especially those pertaining to software and hardware standards. Finally we looked out for general relevant documents utilized in the organization such as competency framework for recruiting employees into the organization and the UN system wide code of ethics. This approach was more useful in decoding some of the espoused values of organizations culture as posited by Schein (2004) such as the published list of values for example what is found in UNICEF’s competency framework.

5.6 Interviews

According to Turner (2010), interviews provide in-depth information regarding participants’ experiences and notion of a particular topic. This position is supported by Creswell (2007) who further said that interviews can be designed to obtain thick, rich data utilizing a qualitative investigational perspective; it can also be used as a powerful form of formative assessment to explore how respondents feel about a particular topic. We rightly used the interview tool to follow up on the participant observation and document analysis. As explained earlier UNICEF has three categories of staff i.e. Management, Professionals and General staff. In the Ghana country Office there are 104 staff members in two locations namely Accra with 76 staffs and Tamale with 28 staffs but we selected to interview 14 employees across the various categories to seek further insight. We conducted the interview over a period of three weeks using 9 days. The interviews candidates were selected based on their length of stay in the organization. We deliberately skewed the selection of the candidates to favour those that had over 5 years stay and had tacit knowledge of the organization’s culture including experience on any historical happenings i.e. the previous staff retrenchment exercise. Each interview session took between 45 to 60 minutes to complete. These interviews gave us much insight into what we set out to look for and ascertain. The interviews indeed provided us comprehensive and quality information that buttressed and gave meaning to observations we had made. We first explained to the interviewees why we were carrying out this interview. We explained to them the purpose of the research
which was to capture the culture of the organization from the perspective of the ten cultural traits that we had deduced from literature review. The interview was semi-structured. We had an open, semi-structured discussion around the ten cultural characteristics taking one at a time. We were guided by questions in the interview guide (see appendix). The interviews were used to elicit the espoused cultural values within the organization according to Schein (2004). A breakdown of the employee population and staff interviewed is detailed below.

<table>
<thead>
<tr>
<th>STAFF CATEGORY</th>
<th>ACCRA</th>
<th>TAMALE</th>
<th>NUMBER INTERVIEWED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>8</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Professional Staff</td>
<td>35</td>
<td>13</td>
<td>7</td>
</tr>
<tr>
<td>General Staff</td>
<td>33</td>
<td>14</td>
<td>5</td>
</tr>
<tr>
<td>Total</td>
<td>76</td>
<td>28</td>
<td>14</td>
</tr>
</tbody>
</table>

Table 5.2 – Interview Table

5.7 Data Analysis Strategy

Yin (2009) proposed five techniques to analyzing data. With regards to this research we utilized the pattern-matching logic approach. The gist of this approach is to compare empirical based data patterns with the predicted one. In our context we matched the data collected from the organization using the various data collection methods against the ten cultural characteristics that we had proposed.

Empirical data was collected along the lines of the different approaches i.e. interviews, document analysis and participant observation. We had beforehand created a chart of the ten cultural traits that we set out to look for. Beginning with participant observation, we placed any information that we observed which related to a particular characteristic into its appropriate column. Whilst dealing with one data collection approach, we kept in mind the three levels of cultural as explained by Schein (2004) and tried to capture where possible, information on the appropriate culture level. For example, Participant observation was a rich source of Artifacts, but as explained in Argyris (1976) “theory-in-use”, it is also a good source of underlying assumptions although further clarifications may be sought on the assumptions to give meaning to them. Document Analysis provided an opportunity to gather some of the espoused values of the organizations such as that shown in the competency framework used in recruitment of employees. We validated the values espoused in this document during the Interview stage where we asked questions to confirm some of the values competencies there such as commitment and communication, which formed part of our theoretical model.

We were largely guided by our theoretical proposition in analyzing and concluding on our findings from our data collected. For example our theoretical proposition required that the organization exhibit characteristics of participation to be positioned properly to achieve policy implementation success. Taking participant observation, we looked out for activities, processes, rituals, procedures, structures, practices and other artifacts in general that could be considered as indicators for the trait of participation. We then moved on to look through documents that espoused these traits. Some of the documents we perused through include, the competency framework, the standards of conduct for International Civil servants and other policy and administrative instructions that showed some sense
of participation inherent in the organization. We then moved on to interviews where we discussed with the interviewees, data we had captured from the prior two approaches as a way of validate and corroborate the information gathered. We therefore basically used the outcomes of the interview to validate our findings from the document analysis and the observation that we had already undertaken.

The results from the document analysis, observation and interviews were also compared to detect instances of variations. Those that were incongruence were further probed to eliminate all biases. For example, we felt that initial observations showed that communication was challenged and that the environment was not conducive for effectiveness communication as there was little presence of “open talk” i.e. a lot of communication at the social level on corridors etc. However we later found out through in-depth observation and interviews that, communication was chiefly carried out through the use of technology, particularly using email and telephone communication. Social communication was also carried out across the telephone that through open communication on the corridors.

In other instances, the analysis process followed an iterative path, moving between the findings from observation, document analysis, and the interview results. This was done to ensure logical agreement and consistency in arriving at results and conclusions. We also consistently questioned and debated our findings to ensure that the basis for our conclusions from the document analysis, observations and interviews were consistent and properly aligned.
6 Results & Findings

The empirical data that was gathered during the study was categorized into the ten cultural characteristics that we set out to find. We also detailed additional cultural traits that were identified to be important to the organization.

6.1 Overall Findings: Per Data Sources

6.1.1 Participant Observation

With one of the researchers being a member of the case organization we had unique insight into their culture. Generally we observed that members of the organization always acted professional in their dealing. This was probably due to the organizational structure were international staff were at the helm of the business units (sections) and the national staff were mainly supervisees except for the units in the operation’s section (one of the two main business units in the organization- the other being programmes section). The organization itself was well structured and governed through the adherence to dutiful work processes by both the local senior management and the global headquarter/regional offices. This allowed for good supervision and control.

Generic administrative policies serves as a strong tool in the culture of the organization and every now and then, policies are sent out through email to all staff members. In line with this, all new staff members, it was observed, were duly initiated into the organization by getting them to go through an orientation session with all unit/section heads and the country representation. This ensured that they had a good picture and understanding of the work culture, among others, in all areas of the organization.

Also informal staff groupings or associations were divided almost sharply along national/ international lines and along operations / programme section lines. This sometimes had a disincentive of creation tension where blame can easily be apportioned to the other party although not necessarily voiced out. This lack of voicing out feelings and opinions is also evidenced in staff meetings where it was observed that people hardly shared their opinions and judgments during discussion sessions. There were circumstances where people have been pointed out reluctantly to edge them to give opinions during discussion sessions.

There is a strong awareness culture on the mission of the organization as the office premises is “bathed” in themes, pictures and posters on Women & Children: the main concern of the organization. This created a strong sense of consciousness on vision the organization was working to realize. There is also a strong use of acronym in the organization which presents a benefit in masking means of statements from outsiders; an aid to securing information and minimizing eavesdropping.

6.1.2 Document Analysis

UNICEF is enriched with a lot of documents that hold information from which we deciphered the culture in the organization. The organization’s intranet holds large amounts of information; an analysis of documents reveals the organization’s Mission and Vision, its position on current issues, policies, instructions and guidelines, annual reports. One such document that binds all persons working in the UN system is the system wide code of ethics for UN personnel. This document contains the purposes, values and principles for all persons working in the UN and it affirms the importance of the UN to secure the highest standards of efficiency, competency and integrity to guide the conduct and the behaviour of personnel (UN Code of Ethics). According to the preamble of the UN, it is imperative for the organization to cultivate and nurture the culture of ethics, integrity and accountability whilst enhancing trust and credibility. In addition to the above overture, the UN as a body is founded on the values of independence, loyalty, impartiality, integrity, accountability and respect for human rights.
Another document that we particularly analyzed was the policies (both those related to information security, human resource and administrative policies). We were opportune to find a document that was particularly useful to our course; this was the UNICEF Competency Framework Definitions and Behavioral Indicators. This document basically defined the values and competencies that the organization believes it and the competencies that it expects its member to process in order to function in particular job roles. It is what is used to assess and recruit all potential employees into the organization and it has also being designed into an interview skill that is taught periodically to selected employees to train them on how to sit on interview panels and also participate as interviewees in employment opportunities. The framework is categories into three sections, UNICEF Core Values, Core Competencies and Functional Competencies. Competency in UNICEF is defined as a combination of knowledge, skills, traits and attributes that collectively enable a person to perform successfully in a given job. Based on these a competency profile is defined to identify specific competencies critical for successful performance in a job with a specific functional area at a specific level. An example is that for a Senior ICT Assistant, who in addition to the core values has the following competencies at level 2 defined below:

- Communication, Level 2
- Working with People, Level 2
- Drive for Results, Level 2
- Analyzing, Level 2
- Applying Technical Expertise, Level 2
- Planning and Organizing, Level 2
- Following Instructions and Procedures, Level 2

The same competency framework is used in performance appraisals at the end of every year to appraise and grade the performance of all staff in using these competencies as requirements.

6.1.3 Interviews

The Interviews were used more to establish and confirm the findings from the participant observation and information uncovered during the document analysis. The Interviews revealed for example that, the seeming culture of non-contribution to discussions in staff meeting was actually an organizational climate that had come about as a result of a recent retrenchment of over 16 staff members at the end of the previous country programme cycle. Most of the casualties were deemed to have been those that made “too much noise”, challenged authority and were generally out of favor with senior management members. We also interviews candidates to confirm their knowledge and experience with the use of the competency framework. Since the competency framework was a recent guideline (less than five years), not very many of the older staff members had gone through it when joining the organization. They however confirmed that they had been part of training sessions to educate them on it whilst others had used it as a guide in their role as interviewers on recruitment panels.

We asked questions concerning their job role and involvement in business processes and decision making and their take on the role and effectiveness of management. Most confirmed their unwillingness to participating in open staff forums as they were of the view, little came out of such contributions by way of its been input into final decisions. Majority confirmed their mistrust for the senior management but admitted that their remuneration (as a way of motivation) was higher than other organization’s in-country. The national staff interviewees were however unhappy about the lack of incentives (allowances) which where enjoyed heavily and by a huge margin by the international staff. An example was cited by one where the rent paid by an international staff for a month was enough to pay for his rent for a two year period.
6.2 Findings: Per Theoretical Proposition

The triangulation of empirical evidence from the three data sources were themed under the ten characteristics as defined in the theoretical proposition and these are discussed in detail below.

6.2.1 Management Style

Our observation and as confirmed through interviews reveal that UNICEF has a flexible management style that is participatory in nature. For example when issues come up for discussion such as the very recent retrenchment of employees in the new country programme (new refined business objectives are set every five years, which require that changes be made in the staffing to support and align with the new objectives), the Senior Management (Rep, De. Rep and Chief of Operations) trickle a discussion and informative style where the issues are first discussed with their immediate supervisees, who then go on to further also hold discussion with their employees. For example, The Chief of Operations holds discussions with the unit heads (ICT, HR, Finance, Admin, and Supply) and the unit heads i.e. ICT in turn hold discussions with his supervisees. Management at the very top is also directly involved with the enforcement of policy at the very low levels. For example as part of emergency preparedness, a radio check (all staff have VHF communication radios to use in time of emergencies) is held every Tuesday at 8:00pm, on the following day, the Country Rep, herself makes time to walk down to each and every person who has not responded to the radio check to gather reasons why he/she could not respond. This approach has gotten the office to record a high level of radio response as they are aware that a no response will mean a visit from the Country Rep.

There is a high sense of proactiveness, particularly when it has got to do with the image of the organization. This is good for Information security and policy implementation since the organization will be most interested in taking steps that will forestall such a thing from happening such as working towards achieving a successful implementation of policies. The highest decision making body, as found out is the Country Management Team (CMT). The membership includes the senior management, section heads, unit heads and a representative of staff association. They together take decisions that are binding on the country office and the entire staff. Of course, whatever decisions they take are within the framework of the organizations policies, rules and regulations.

As with the recently introduced VISION project (ERP system), the Chief of Operations lead the project, in addition, champions were elected from each of the major sections to be trained and to assist with the implementation process. The project got an operations officer post created who worked directly and closely with the chief of operations purposely for the VISION project. There is a strict reporting structure to follow up on the progress of initiatives and projects and this is laced with periodic meetings to discuss the way forward. These meeting are also consultative in nature and allows for people to contribute to decision making such as on the approach or methods to pursue particular tasks. Largely however the big decisions are left to the senior management. The consensus arrived at from the interviews were that hierarchy between regular staff and management was alright, it must be added also that an open door policy is informally practiced making it easy to approach all members of the top management.

We got the general impression that management was dutifully involved in the activities of implementation and adopted a more open approach to taking decisions. The open approach also meant anything that happening in the country office was more likely to be known at the regional office or headquarters level, which had oversight responsibility for the country office. Management was also highly proactive on issues concerning the image and security (with emphasis on personnel security) of the organization. UNICEF showed a management style that was supportive and involving which is good for security policy implementation.
Taking Detert’s (2000) organizational culture dimension into perspective particularly, our findings revealed that an organization successful with policy implementation was more skewed towards the collaboration side of the Isolation vs. Collaboration Dimension. Empirical data also revealed that unlike Fung & Jordan (2002)’s theoretical assertion that management left the responsibility of Information security measures to IT, UNICEF had a governance framework that was driving the need for information security. This is in line with Lim et al (2009) assertion that security matters are taken further up the organizational ladder. The open nature of the environment allows for some contributions to be made to decisions either formally or informally. The top management also has a tendency of demonstrating concern for security issues (usually personally security issues and this easily transcends to security in general including information security) which is duly followed by the rest of the employees. This is in alignment with Hone & Eloff’s (2002) claim that the tone of security needs to be set at the top in order to establish the right attitudes.

### 6.2.2 Trust and Responsibility

UNICEF has a number of information technology/security policies such as the electronic code of conduct, computer disposal policy, password policy, information disclosure policy (formerly information security policy), backup policy, software acquisition, classification and certification policy, physical and environmental policy etc. Most of the policies that were analysed have a Responsibility Section, which details the individuals, units or locations liable to performing, carrying out or adhering to the relevant portions of the policy documents including the exact functions to perform. Example of the components in the policy documents are the Approver, Policy Manager, Responsible Unit, Audience. These components are evidence of a strict culture of responsibility as well as management and supervision.

Responsibility strictly in concordance to as provided in the employee’s job roles is a lifestyle in UNICEF. There was a high sense of everyone understanding their role to get the job done. There was less incentive for employees to necessarily develop new techniques or procedures to perform their job tasks as job roles and procedures are largely defined and have been established over the years. For example the operations section has a guide of standard operating procedures which most employees prescribe to, in order to carry out their tasks. Of the few interviews we did, only those in supervisory positions had the responsibility of formulating projects, most were however mostly directly involved in the implementation of projects by way of small activities that they perform. Because job roles are highly defined it is difficult for one not to take responsibility for bad actions and in fact most respondents confirmed this. However on the responsibility for good actions, everyone confirmed that the result of good actions is shared among the team. Respondents were also divided on the issue of being burdened with the problems of the organization. The feeling of trusting management to take decisions in the interest of employees was however absent. The good aspects, which were really relevant to the research was that there was a strong evidence that all employees understood their job roles and what they each had to do to get the entire job done and the organizations objectives met.

In UNICEF, all staff are aware of their job descriptions and they develops their own work plans yearly albeit with their supervisors as part of their performance evaluation reporting. In doing this, they are allowed to develop their own work practices (within the larger framework of the existing work policies and procedures) to meet their performance targets. This style according to Dhillon & Backhouse (2000) ensures that employees understand their responsibilities when met with unusual situations and it also fosters trust as there is a lessened external supervision. A high sense of ownership is developed within the employees because of this approach. The leeway given them to develop their own work
plans is as confirmed by Dhillon & Backhouse (2000); evidence of trust that they will abide by the organizations rules and norms.

6.2.3 Bureaucracy and Dependencies

The organization employs a rigid procedural approach to carrying out tasks as part of its daily operations. The main ERP system (SAP) from which most of the organizations transactional tasks are run in, has a lot of internal controls that require segregation of duties and this also applies to manual procedures that are carried out, outside of the system. There is confirmation through the findings of observations and interviews of a strong procedural culture, roles are highly segregated to the smallest grained level possible, requiring a dependency on a number of persons to complete a single task. Activities and routine tasks all follow laid down procedure. The staffs are used to carrying out their various and diverse tasks in a bureaucratic manner and hence the introduction of new policies such as information security policies, (which many see as very bureaucratic in nature), are seen as normal within the UNICEF Ghana fraternity.

With this organizational attribute, staff of UNICEF naturally and largely follow procedures and policies and although this course has the tendency to lead to a pursuit of processes rather than speedy results, results are ultimately achieved. In this regards, respondents were quick to admit to the organization being process-oriented as opposed to results-oriented.

This culture of bureaucracy and process-orientedness is however good to allow a strict following of policy implementation to achieve results. A culture that has weak bureaucratic tendencies has the possibility of encouraging by-passes which is detrimental to information security and policy implementation in general. Respondents were very aware of how they contributed to the achievements of the organizations objectives. The strong evidence of bureaucracy and dependability as evidenced in UNICEF is seems to be beneficial for information security policy implementation.

The empirical findings reveal a leaning towards Hofstede’s (2011) process-orientedness as against results-orientedness, in his organizational dimensions of culture. As rightly explained by Hofstede (2011), UNICEF’s work culture is dominated by bureaucratic routines and a need to dutifully follow processes sometimes at the peril of achieving results. Power structures were however not dominant in the work culture as put forth by Hofstede (2011) where he explains it as being an inhibiting factor to the smooth implementation of processes.

6.2.4 Motivation

Motivation can be explained from the perspective of the reward systems that exist in the organization. Generally, there is some sense of casualness that exists particularly with attitude towards attire and also the early closing hours. This can be a strong incentive for employees as people are generally more social and will enjoy these benefits against working in a more highly formal setup. The comparatively higher level of remuneration compared to other organizations (in the country at least) also remains a motivation factor. Working with UNICEF and the UN in general is seem as prestigious and workers do well to identify themselves with the organization, including other privileges that come with the territory such as use of the organization’s diplomatic passport which gives one elevated privileges when travelling. Motivation was observed to be very strong throughout the organization but this was strongest especially with the programme staff who work directly with women and children (whose rights remain the concern of UNICEF). Most of these groups of staff (who are social workers anyway) have a strong desire to work for the good of women and children; this motivation is however also...
supplemented with the frequent travels into the field which comes with the monetary rewards. It must however be said that the operation staff made up of ICT, HR, Finance, Admin and Supply) remain less motivated as they do not work directly in relation to the core objectives and mandate of the organization of protecting women and children. There are also less travels for such staff which as mentioned come with its monetary gains. Respondents generally felt they were well-resourced to perform their job functions, they however largely confirmed that they didn’t need to be motivated by the rewards or performance of their fellow colleagues but admitted to a pressured work environment boosting but not necessarily inspiring them to perform more. On the special reason to work with the organization the two management members admitted to being motivated to work for children, the professionals and general staff largely confirmed that the monetary motivation was key reasons for their continual stay in the organization.

UNICEF (and the UN) has recently been the target of external attacks and because of this there has been a lot of emphasis on personal security. Because issues of security directly affect the staff members themselves, staffs are highly motivated in this regards to support security initiatives. An example of this is the willingness to abide with security scrutiny and checks when entering the premises every morning. Respondents also felt their views were duly considered where they had made valid points or contributions.

Largely, staffs are highly motivated to work in the UNICEF environment and it is generally good to have motivated people work towards implementation projects/programmes such as that for information security. The motivation exhibited by the organization serves as a boost to successfully achieve results with ISP implementation.

Ruighaver et al (2007) rightly suggested that staff motivation is increased if their contributions on security are duly considered as was the case observed in UNICEF. During the various periodic meeting suggestions are usually collected and factored into the decision making process and this actually enhances the implementation of processes/programmes such as information security. The open door policy that exists in the organization is also evidence of mainly vertical but also horizontal social participation as theorized by Ruighaver et al (2007). Horizontal participation enhances discussions among staff within sections and units whilst the vertical participation ensures that formal suggestions about security climb up the organizational hierarchy such as during meetings.

6.2.5 Budget and Funding

Implementing information security policies requires budgeting and financial support to be successful. This we saw as a critical value within UNICEF where projects and activities are adequately budgeted for and fully funded.

The organization operates under a country program cycle of five years, where funds are allotted from headquarters to execute programs under the umbrella country program over the period. For the entire country program there are results that need to be achieved for the programs and a set amount is allocated for each program. The results to be achieved are called PCR: Program Component Results. Under each PCR there are intermediate results: IR, which are individual projects that need to be carried out and aid towards achieving the PCR. Funds are allocated for each of the IR’s as well. Now under each IR, there are a number of activities that also required bringing success to a particular project. Each of these activities also has funds allocated for it. A breakdown of funding sources for all tasks is therefore a combination of PCR, IR and Activities which is known as WBS: Work Breakdown Structure.
At the beginning of the year, funds are allocated (based on prior discussions with supervisors and team) to all sections/units including the ICT unit to do a supply and procurement plan that includes all expenditure including that to be spent on information security and its associated services. The funding for this plan is supervised and approved by the chief of operations who is the oversight supervisor for head of ICT unit. Funds are available for specific expenditures as part of the activities which feeds into the IR and therefore the PCRs. All funding is therefore preplanned and structured to be made available to all projects and activities including information security policy implementation.

For example, for the ICT unit to make any particular expenditure, it contacts the operations assistant: who assists the Chief of Operations to manage funds for the section. The operations assistant who is the budget holder, provides the appropriate budget line to charge the expenditure to, mind you the budget is broken down into lines as explained above.

There is a chart of accounts which details how funds are treated, that is whether they are Assets, Liabilities, Revenues and Expenses. Under each of these classes there are subclasses that also detail the exact type of say revenue or expense with their appropriate codes. For example under Expenses, there is a section for communication services and under this; there are specific allocations of funds for various types of such communication services. Telephony for example comes with an expense code of 7110210 whilst Emergency Telecoms has a code of 7110220. All expenditures are therefore strictly funded, allocated and spent accordingly.

Because of the structured nature of funds allocation, one can be assured that if already properly planned for and discussed, there will be funds allocated to carry out any project or activity such as the implementation of an information security policy.

UNICEF being funded by governments and private institutions and individuals remains largely appropriately funded to carry out its programs. The structured nature of the budget and funding also ensures that spending remains within what is planned for. It is difficult for any section/unit to overspend its budget. Budgets are strictly monitored and are diverted to other accounts only when they are underspent. The structured funding mechanism in place actually makes it one of the strengths of UNICEF.

As stated by Al-Awadi et al. (2007), Whitman & Mattord (2009) and Dinnie (1999) that appropriate budget and funding is critical to the successful implementation of information security policy, our findings revealed that budgeting is a dominant and an appreciated culture in UNICEF. Although information security has been described mainly as a human problem, we believe achieving information security is an equal combination of both the necessary tools (software, hardware; which requires budgeting and funding) and human factors. In this direction, we found UNICEF to have provided adequate budgeting and funding for all IT and information security related issues. This confirms the assertion by Al-Awadi et al (2007) that resources in organizations are the foundation requirement to enforce, monitor, implement and achieve information security.

6.2.6 Awareness, Education and Training

Email remains the main medium by which awareness is carried out. The ICT unit for example has the approach of regularly sending information related to security advice and tips on ICT in general to staff. This practice also exists at the global level i.e. ITSSD (Information Technology Services and Solutions Division), who regularly send security alerts through a global broadcast to all employees about security threats, vulnerabilities and information on malware in general. The ICT unit however does not regularly organize training for staff, this is done occasionally with reasons among others being that the entire organization is more geared towards a culture of self-learning were a lot of learning material is
available on their web portal and all staff are expected to go there and self-train. The organization also has partner organizations to provide training on areas such as leadership, management etc. This approach applies to almost all staff including ICT unit who are only rarely sent on external technical learning events or the once a year regional workshops where ideas, issues and new initiatives are discussed with other ICT colleagues from other country offices.

There is a robust awareness strategy in UNICEF particularly concerning its mandate of advocating and protecting the rights of children where staff are inundated with images of children and women. All workstations come with custom made active desktops and screen savers that are continually showing the images of children and women in need and in their plight. The office premises also has a lot of printouts and images of children and women and this is a powerful tool for creating awareness to the plight of women and children and the need to assist them. Since this culture is strong and already been lived, it can very well be easily adapted to issues related to policy implementation to enhance effectiveness. Our observation and interviews largely confirm that staff are confident about the level of information passed down to them concerning issues of security particularly through email although they admit to a limited existence of active security training.

Most respondents cited the recent example of the implementation of the ERP (VISION) system when making references to being informed about projects. The VISION project was well managed in an efficient manner. External in-house training was provided for a select few (champions) who then returned to train other staff. Alongside these, there was an entire system developed to provide web based training in all the country offices including Ghana which are housed on premises. The system has all the tutorials and learning materials including audio, presentations, demonstrations and video and these are periodically updated with new information. Online trainings are also organized on demand, by subject matter experts from the global headquarters for specific areas where further understanding is required.

All respondents confirmed, as noticed in participant observation, to going through an orientation program with all the sections and units and these usually involves discussing some of the pertinent policies that guide the section and therefore the organization’s practices. The ICT for example discusses at length the contents of some of the policies particularly those related to information security such as the standards of electronic conduct, information disclosure policy, access control of UNICEF’s information assets and password policy. The Admin and HR units also take new employees through policies such as MOSS (Minimum Operating Security Standards) compliance, security in the field, staff rules and regulations, financial disclosure and declaration of interests and standards of conduct for international civil servants.

External professional training goes through a rigorous system of approval, certifications and board reviews and this practice discourages most staff from seeking to enhance their professional skills in this direction. The organization chooses to encourage staff to self-study using its internal online / web based training systems such as “skillport” or partnerships it has created with some leadership training institutions. This makes employees only relevant to the organization and its systems and one may find the skills of such employee severely limited in the outside world. In-house refresher trainings are limited with the ICT unit for example not carrying out more than two trainings for staff in a year as most education are by way of awareness tips through email. Funds are also budgeted for internal training sessions but these are minimal since most of these trainings are done online. Most respondents did not agree to being necessarily obliged in the strictness sense, this was because, such trainings directly had an impact on their ability to complete their tasks and this motivated them to willingly attend such trainings. The few formal in-house trainings that are carried out are not categorized along the lines of employee type and the rationale behind implementations are duly brought forth if not they are inquired by the employees themselves.
UNICEF has a somewhat appreciable training and awareness system but these as mentioned are geared mainly towards in-house developed or external partnered training institutions. Formal trainings and refresher tutorials, even by the sections and units are however limited and there is a heavy reliance on self-training and development. Although the encouragement of professional training is weak, it fashions its awareness and trainings appropriately to in-house projects which in some sense is what is being sought.

Contrary to the suggestions by Al-Awadi et al. (2007) that training and awareness programmes should be carried out based on job type and employee level, the empirical evidence on the ground shows that the little training and awareness that is carried out bundles all employees together. The frequency of contact-based training was however low with heavy reliance on email and other electronic information sources as the main tool for information security related communication and awareness. This practice is however in tandem with ISO/IEC’s (2005) suggestion to organizations to make their employees aware about security matters in the course of their daily works. Keeping in line with Whitman & Mattord’s (2009) suggestions, the ICT unit periodically sends and informs employees about information security policies as a way of keeping it fresh in their minds. Although not carried out as a contact-based training & education, this awareness approach of regularly sending email security information and alerts is also congruent to Dhillon’s (1999) recommendation to perform it on a continuous basis in order to achieve the expected outcome.

Taking UNICEF’s regional and HQ office hierarchy as a governing board, the practice exists where local management periodically update and inform the board on security matters in the country office, which is in line with Lim et al’s (2009) submission.

6.2.7 Participation and Cooperation

The organization employs a number of IT based tools to enhance and improve upon cooperation among employees. Apart from the email, which is the cornerstone of all communication in the country as well as global organization, it uses Yammer: a corporate based social network application to foster participation and communication across function and geographical lines. The Yammer has various groups which enjoy an appreciable level of participation but it has been most successful with the introduction of its new ERP system (VISION) where ideas and information are shared across this platform.

When new global wide applications are to be implemented, it tries to foster participation and inclusiveness by inviting participants form all regional areas across the world an example being with the global VISION trainings that have gone on during implementation. The travel by staff members (which of course comes with some per diem “motivation”) may be described as serving some form of motivation and so it the opportunity to travel itself. Most implementation initiatives already require people to work in teams. This practice is also evident during training sessions where there is emphasis to carry out a lot of group work exercises. Generally there is cooperation on the implementation of projects but it is however evidence through observation and interviewing respondents that there is a limited contribution during meetings. There is a sense of insecurity particularly among national staff, who are circumspect in their contributions in meetings so as not to unnecessarily slight their supervisors who are mostly international staff. The nature of employment means all staff are on a two year renewable contract subject to availability of funds and need for the position. This circumstance creates a sense of anxiety on staff to be circumspect. Conversations are carried on to the corridors and sidewalks instead of being discussed during meetings. Management has however on numerous occasions encouraged the discontinuation of such a “silent” practice in meetings with little improvement. A management change is imminent and this may be able to determine whether this
climate can be gotten rid of if a new set of management takes over. Participation in meetings particularly with regard to decision making is therefore left challenging.

This climate of the organization can partly be traced to a recent retrenchment of staff during the recent country program which saw a lot of national staff losing their posts. The practice can also be traced to the national culture in Ghana which discourages supervisees confronting or countering the views of their supervisors. The cultural trait exhibited here is a clear case of a clash between national culture and organizational culture and it is also a classic example to distinguish between an organizational climate and an organizational culture. As explained earlier the current climate is as a result of an event that has taken place in the organization which has tended to affect the behaviour and feelings of employees. Culture is however a more permanent feature.

Participation of employees in other activities such as training sessions and retreats however is strong and this makes them feel important and part of the process. There is a lot of involvement in such activities and adequately cooperate with each other. There are periodic meetings between members of staff as part of different groups. There is the CMT (Country Management Team) which is a representation of senior management, all section and unit heads and representatives of staff association, the CMT meets once every month. There are also the Programme-Operations meetings; the two main divides of the organization to bring forth and discuss challenges and bottlenecks and how best the two sections can support each other to enhance meeting the objectives of the organization. These meetings serve to foster relationships between the two bodies and they occur every quarter. Members of the Sub office in Tamale are joined to such meetings through online web and audio conference connections. The is also the Operations Unit head meetings which are held in the first week of every month between the Chief of Operations and the supervisees unit heads of Admin, Supply, HR, Finance and ICT, to discuss pertinent issues at hand and also the tasks and activities been currently pursued by the units. This meeting is also called on a need-to-have basis at the request of the Chief of Operations. The units, such as ICT also hold their own meetings but these are purely at the discretion of the unit heads. There is also a general operations meeting for all operations staff which is called once every quarter where all issues in the operation section are brought on board and discussed. All such meeting are obligatory and non-attendance can go against one in his or her performance appraisal at the end of the year. One will find that staff are more likely to communicate and speak freely during such smaller meetings but as explained earlier, this is not the case during the larger meetings where all (including senior management) are present. Most implementation activities on projects usually involve participants within a section but from different units but there are the occasional ones that require cooperation across sections. There are instances where viewpoints of lower end staff are considered during such meetings with decisions being reached on consensus; these however do not apply to the big decisions. These decisions are only discussed in a superficial manner to give and impression of consultation but they are usually already taken.

Participation and cooperation is highly encouraged by senior management but as explained the current climate has inhibited appropriate participation particularly in decision making meetings involving all staff. Implementing security policies needs the participation and cooperation of everyone to be successful. This organizational trait needs to be improved upon to bolster and successfully contribute to the implementing information security policy.

Our observation revealed that employees in UNICEF tend to contribute to issues when they are in smaller group settings. This is in direct agreement with O'Reilly and Chatman’s (1996) findings that employee’s participation in group activities or decision making makes them feel important and increases their effort to ensuring success. The resultant effect is that employees believe they have contributed to and are therefore an integral part of the resulting decision as a result of their contributions to issues and are therefore bound by them. Also the encouragement by management on participation and
cooperation collectively represents the viewpoints of different parties to reach consensus which has been argued out by Flechais and Sasse (2009) as a key element to implementation.

6.2.8 Commitment

Most of the workers, particularly the programme staff are very committed, towards their work. As explained by them in interview discussion, this is because of the satisfaction gained from helping and protecting the rights of women and children. There is generally some sense of enthusiasms when employees are identified to be working with such an organization and this serves as a catalyst to keep them committed. Respondents saw themselves as part of the organization with most of them largely agreeing with the values of the organization. Some respondents however brought to the fore that some of the values preached by the organization which were not been applied when it came to employees. An example was cited by a national staff respondent who on discussing the differences in remuneration between national and international staff highlighted some incentives that were not available to them. He brought up this discussion in the light of the organization championing its human right principles of humanitarianism, equality, neutrality and impartiality and wondered how equality juxtaposed against international staff been incentivized differently. Of course, some of the responses to this inquisition that we gathered was that the international staff were not native to the country and there was a need to make them some comfortable as possible.

Of the respondents we interviewed, they were generally of the view that the positive feelings they had towards the organization will be replicated only if they found themselves working in an organization with similar values and objectives. They were also similarly committed to put in extra effort to help the organization succeed.

Commitment is of such importance to the organization that it is listed as one of the three core values of the organization. UNICEF defines an employee as commitment if (s) he “Demonstrates commitment to UNICEF’s mission and to the wider UN system; demonstrates the values of UNICEF in daily activities and behaviors; seeks out new challenges, assignments and responsibilities; promotes UNICEF’s cause”. Generally, working with the UN is more rewarding in terms of remuneration and could account for an appreciably high level of commitment. One gets the sense that, commitment may largely emanate from the remuneration irrespective of whether employees believe in the values of the organization or not. It is our notion that if commitment can be attained irrespective of whether employees believe in the organizations values or not, it will still work towards meeting the objective that is set out. The only setback is that the incentive for the commitment has to be continually refreshed.

The UN, and for that matter UNICEF’s environments is rife with the social pressure to behave in a manner as dictated by the organization’s culture. As explained by Pahnila et al. (2007) this attitude is good for ensuring compliance, which is a major cornerstone for adherence to information security and this ensures that policy gets to be implemented with minimal resistance. To a rather large extent, people’s feelings with regards to association with the organization and acceptance of the organization’s values as defined Pareek (2004) are well established. This willingness and feeling towards the organization is a good driving force to ensure that security policies are followed and implemented as outlined by the organization.

The willingness to exert high levels of effort on behalf of the organization (which comes with some expectations for return), Luthan (1995), serves as a strong point to ensure that roles and responsibilities assigned in the implementation of information security policies are dutifully executed. This effective carrying out of roles and responsibilities is further buttress by Hellriegel (2001) who also claim that the
commitment goes beyond loyalty to include active contribution to accomplish organizational goals in this case information security.

Following from the definitions and findings, we will define this attribute as the employee’s innate desire & willingness to accept and ensure that the security goals expressed in the information security policy are achieved

6.2.9 Communication

Communication is closely tied to the participation and cooperation that has been discussed above. Regular meetings form the culture of the organization. This trait is therefore discussed in the perspective of that other trait in terms of meetings that serve as opportunities for communication. As explained above, there is the CMT (Country Management Team) meeting which is held once every month where all issues relevant to the organization are brought up and discussed. There are discussions of issues ranging from general security and risk issue to employee welfare. The decisions taken at this meeting are binding on all country office staff. The minutes of the CMT meeting are made available to all staff. This assembly which is representative of all section and unit heads including the Country Rep, Dep. Rep and Chief of Operations is the final decision making body in the UNICEF country office and it serves as a platform for horizontal interaction between sections and the units. It also serves as vertical interaction and consultation between the section and unit representatives and their supervisors including senior management.

There is also the programme-operations meeting which is held every quarter to discuss and resolve issues and bottlenecks between the two main sections of the office i.e. programmes section ad operations section. The Operations section (HR, Finance, Admin, ICT, Supply) mainly function to serve the need of the programme section to enable them meet their mandate of advocating for the protection of the rights of children and women. There is also the monthly meeting of the operations unit heads where all the unit heads under the section meet with the chief of operations for them to discuss their program and schedule of activities including issues of general concern. The operations section in totality also meets once every quarter, and all section members both unit heads and all supervisees discuss both functional as well as welfare matters. As mentioned earlier the Email system remains the prime mode of communication and one finds any pertinent information been sent through this medium, this includes announcements and decisions taken for example at CMT which is forwarded by the country Rep to all staff.

Respondents confirmed that generally, information is communicated effectively with colleagues and supervisors for them to effectively carry out their tasks. Most of the other documentary information required to perform ones tasks is also availed on a shared drive (N - drive) operated in the country office. The shared drive categorizes the information alone section/units and topical themes such as Policies and other security information. Information is also available on the organizations web portal for one to perform his/her tasks. For example the intranet hold information on the current specifications of ICT equipment that make up hardware standards and this can be easily retrieved from the supply section of the portal. The ICT unit retrieves the specifications and pricing from listings of global vendors that the organization has agreements with. They then use this information to create purchase requests for equipment required which is then forwarded to the supply unit for further processing. There is also the SOP (Standard Operating Procedure) manual that details how to carry out the transactional activities in the units of the operations section and this serves a major source of information. Regular updates to these are sent through email notifications. Staff are well aware on how to access these information. Largely, the organization operates an open door policy, literally and therefore one can be able to walk into the offices of supervisors including the Country Representative to discuss pertinent issues, although prior information is required for other more serious and lengthy
discussions. This practice is particularly good for communication among staff. Communication in meetings is however stifled as explained earlier because of the current organizational climate and historical event of retrenchment. It has also been explained by the cultural preference of the nationals. Respondents also largely believe that communication with management is adequate and that information is freely communicated where necessary.

To highlight information that might affect ones job been communicated in a timely manner, an example can be cited of the recent retrenchment of staff in the new country programme exercise. Because of the sensitive and dispiriting nature of such an exercise, there was active communication and counseling sessions with the affected staff and they were actually informed about nine months prior to their departure.

With regards to the initial reception of staff, quoting one respondent, he said right from the time he started the recruitment process till he finally got the job, he was received very warmly and it was one of the best, if not the best receptions he had had in any recruitment exercise. He said this kind of reception actually helped him to relax and feel less tensed during the interview stage. He confirmed he also had a good interaction with the Human Resources unit during his initial days and orientation with the unit.

Figure 6.1 – Top level Hierarchy of Shared (N) Drive – Used for Communicating and Sharing Information
Communication is of such importance to the organization that it forms one of the three core competencies of the organization which all employees must possess to be working in the UNICEF environment. These three competencies (Communication, Drive for Results and Working with People) are not just listed or published values; in fact they are used in the recruitment of all staff where the interview panel is provided with indicators by which to establish the communication level of prospective employees. It also forms part of the yearly performance appraisal system where supervisors must grade their supervisee’s performance in this regard. See a portion of the Competency framework showing the indicators for communication below;

<table>
<thead>
<tr>
<th>C O M P E T E N C I E S</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Competencies</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Communication</td>
</tr>
<tr>
<td>Level 1</td>
</tr>
<tr>
<td>Speaks clearly and audibly.</td>
</tr>
<tr>
<td>Clearly explains information.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------------------</td>
</tr>
<tr>
<td>their reactions and feedback; projects credibility; structures</td>
</tr>
<tr>
<td>information to meet the needs and understanding of the intended</td>
</tr>
<tr>
<td>audience; presents information in a well-structured and logical</td>
</tr>
<tr>
<td>way.</td>
</tr>
<tr>
<td>Checks that others have received the general message when</td>
</tr>
<tr>
<td>speaking to them.</td>
</tr>
<tr>
<td>N/A</td>
</tr>
<tr>
<td>Structures information in a straight-forward fashion.</td>
</tr>
<tr>
<td>Adjusts the amount and degree of detail of information for the intended audience.</td>
</tr>
</tbody>
</table>
Table 6.1 - Communication competency Extract from the UNICEF Competency Framework

UNICEF’s open door policy and easy access to the topmost hierarchy is in alignment with Ruighaver et al’s. (2007) encouragement of social participation along vertical and horizontal lines. This is also in line with Hofstede’s (2011) open system dimension which refers to the common style of internal and external communication and the ease with which outsiders and newcomers are admitted. Significant use of emails and shared information portals to disseminate security information among others, counters Ruighaver et al’s (2007) scenario where employees at the same level within different areas may not be aware of the same critical security issue.

The scenario of diffusion of responsibility; two different employee groups or individuals assume that an issue is the responsibility of the other, as described by Flechais and Sasse (2009) is clearly annulled in the UNICEF environment. This is because there is an extensive use of shared documents and templates that clearly assign and report the responsibilities and tasks to be performed by individual. For example, apart from the job description documents that is availed through the shared portal by the human resources unit, there is the use of performance evaluation reporting (PER) to document, communicate and discuss the responsibilities of individuals in conjunction with their supervisors and this is referred to by them periodically to ensure that work plans assigned over the period are dutifully carried out. There is also for example, the existence and the use of a “work plans and key assignments” document template that must be updated and reviewed before the periodic coordination meetings and this enumerates the individuals the assigned tasks and the completion rate of tasks by the month. These practices together with the periodic meetings themselves ensure that all issues are discussed and as put forth by Kolkowska (2003), curiosity is minimized. In relation to security implementation, such practices that are already in place will ensure that the necessary communication that needs to effected to ensure successful implementation is achieved.

6.2.10 Supervision, Co-ordination and Control

Analysis of the documents available reveals a rigid and well-structured organization that ensures proper supervision and control. The structure both in country and globally is that all supervisors (sections heads and Sr. Management) are international staff and the local staff make up the rest of the professional category and the general staff. This structure has encouraged a culture of non-collusion, and strict supervision. The global structure (with the prime headquarter at New York) also creates a halo effect where anything coming from the headquarters is seen as sacrosanct such as the case with information security policies (and policies in general) been distributed down to the country offices. A policy administrator exists at the headquarters in New York but at the country office level, the ICT Unit head acts as the one responsible for disseminating and educating on policy and he is responsible for the overall implementation of policy at the country office level. He is also responsible for developing local ICT policies and is also part of the country management team, which is the final decision making body in the country office.

All policy documents of the organization clearly states the punitive actions for flouting of policy but specific issues such as punctuality and timeliness are generally lenient.

Implementation plans are usually accompanied by a procedure to follow up on progress and it is followed through procedurally with haste not compromising the process.

The maximum steps between any staff member and the country representative being the topmost of management is two levels and this allows for proper oversight by senior management. All sections heads have the country representatives as their immediate supervisor and unit heads have the Representative as their second reporting officer. The organization is well structured, can be described
as distributed and is organized around the main business objectives of programmes; who work directly to fulfill the mandate of UNICEF and Operations; who work to support and enable the activities of the programme staff. The organogram is structured enough to allow for concrete and rigid decision making and at the same time flexibility enough to allow for easy and quick decision taking. By and large UNICEF organogram is well structured and efficient allowing for proper supervision co-ordination and control to enable the taking of right decisions and prevent bypass of procedures and processes. It cultural traits is good for proper implementation of information security policies.

In line with Whitman & Mattord’s (2009) discussion for selection a security champion, UNICEF also as mentioned has a policy administrator at the global level. At the country level, this is the focus of this study, the ICT unit head acts to function in this role. Although most of the policies have already been developed at the global level, there are a few that come in the domain of the country ICT unit head such as a local telephone policy and backup policies. The unit head acts to create, distribute and enforce these policies as well as those coming in from the global level. Supervision and control is already reflected directly in the management of ICT resources by the ICT unit such as the distribution of workstations and installation of software & applications, disposal of obsolete computer equipment etc. all in line with policy guidelines. The organizational culture already understands that the ICT unit “dictates” all technology implementations and the organization in turn reposes this trust and responsibility into the hands of the ICT unit as explained by Whitman & Mattord (2009).

The organization, by its culture, in other spheres of security such personal safety already understands and has embraced the need for security related decisions to be supervised and controlled by an individual or group of persons although there is room to allow for meaningful contributions. This position is buttressed by Ruighaver (2009) et al in their explanation that dependency of security culture makes it impossible to a tight security culture in a loosely controlled organization and vice-versa. There is tight control over security processes and policy and monitoring is also evident.

These ten cultural traits will be to successful ISP implementation just as standards are to Policy itself. Effectively, the ten cultural traits will be norms i.e. standards by which the organization will be guided to successfully implement ISP’s from a cultural perspective. The role of organizational culture in achieving successful implementation of information security policy is in its ability to appropriately define and inculcate normative behaviours that will ensure, employees follow instructions and directives that are spelt out by senior managements in the policies print & ink.

6.3 Other Findings

Apart from the particular cultural characteristics that we set out to identify and confirm, we also came across some cultural traits that we thought were highly pertinent to information security policy implementation and information security as a whole. These traits were also confirmed by some of the respondents when we asked them to confirm the existence of other characteristics they thought were evident in the organization. The characteristics are possible candidates to expand on our theoretical proposition and it will require further research in the future to establish these. The traits are discussed below.

6.3.1 Integrity

Integrity is strongly stressed in all dealings and there is the expectation for all staff to exhibit this trait. All throughout conversations, meeting and policy statements, there is the ascription of Integrity to
staff, which places a burden on them to behave and act in a manner that the organization expects. An example of this is where at the end of every month staff using the organization’s cell phones are sent their bills, with the request to tick and make payment for private calls that was made with the phone. The staff of course has the choice to select only a few calls to pay as private but the burden of integrity instigates a culture where most staff do the right thing. But of course the expectation of future audit and its associated sanctions may be responsible for staff behaving in this manner. This is evidenced by the strong disciplinary culture where penal actions and administrative measures that are meted out are periodically sent out by the executive director himself though a global email broadcast to all staff. The offences that warrant these sanctions include illegal medical claims, watching of pornographic material after work hours and unauthorized use of organization assets and information to facilitate personal gains. The sanctions include dismissals, demotions, Salary fines etc.

6.3.2 Ethics

We realized that ethics was a strong trait that was exhibited in the organization. There is solid defense of what is right from wrong i.e. ethical behaviour and proper conduct among others. These ethical requirements are defined in the standards of conduct for international civil servants. There are also a number of ethics related documents, including, the system-wide code of ethics, Oath of office and UN charter that assist with this agenda. There are also policies on the Acceptance of “Awards, Decorations, Gifts, Honours, Medals, Remuneration, etc.”, Anti-fraud Policy, Whistle-blower protection etc. The organization also employees a number of tools and approaches to nib unethical behaviour in the bud including a financial disclosure survey tool that is completed by selected staff (especially those occupying higher level positions) every year and ethical behaviour trainings. Information Technology also has its share of ethical requirements (some of which form part of ICT policies) including direction on the access and use of organizational systems like electronic communications, data storage, retrieval equipment, software and internet usage.

UNICEF has an independent ethics office, headed by a principal adviser who reports directly to the executive director. It is primarily responsible for cultivating and advancing management and staff awareness of UNICEF standards on ethical behaviour, and proper conduct among others. It also advises management to ensure that UNICEF’s policies, standards, procedures and practices reinforce and promote the ethical standards and they are clearly understood by all.

6.3.3 Language

One major observation in the UNICEF Ghana office (more probably globally) concerns language. There is a substantial use of acronyms and mnemonics in UNICEF. This is good for general information security implementation in that it makes it difficult for outsiders to discern any tacit knowledge that is being inadvertently been divulged by employees. It eventually works towards achieving protection for information in that communication that is carried out in the organization is “encrypted” and not easily understood by outsiders.

6.3.4 Heroes

During the research, particular the interviews, one hero in UNICEF came across as know by most employees (even if they don’t grasp his story) was Jim Grant. Jim Grant had dedicated his life to the cause of protecting and developing children and his approach and deep passion towards children has inspired many an employee, especially the programme staff ( and particularly the international staff, who work directly for women and children) to strive towards finding solutions and working for the
advancement their cause. This case across a lot with most of the programme staff that we talked to during the interviews and there is also a lot of reference to his name when appeals are being made towards the course of women and children. We also came across his name from references during document analysis.

### 6.3.5 Guidelines

There is also extensive use of guidelines in UNICEF and this perhaps contributes substantially to the success of implementations. For example in the ITSS Division, every IT project that for example involved the migration or introduction of a new system is accompanied by a very detailed documentation meant to serve as guideline for installation, updating, configuration etc. IT personnel therefore literally follow the instructions in the documentation to effect the implementation of a server system or application. The heavy reliance on documentation guides can therefore likely to be a possible reason why there is good success with the implementation of IT systems. This situation can therefore be easily analogous to the implementation of the information security policy.
7 Discussion, Conclusion & Further Research

7.1 Discussion

Among the objectives of this study is to bring to the fore, particular cultural characteristics that can be adopted or adapted by organizations to bring success to the implementation of their information security policies. The core objective of implementing information security policies is to influence employees to behave, act and think in ways that go to protect the information assets of the organization (Whitman and Mattord (2009), Höne & Eloff, (2002)). To do this, one must work to find out what influences employee behaviour in the organization. When this is found, we can estimate how it will impact on and lead to achieving success with information security policies. This line of thought notwithstanding, it is nonetheless also important to highlight the many factors that generally influence the behaviour of people and employees for that matter.

According to Hofstede (1993), for people living within the same social environment e.g. organization, it is important to differentiate culture from personality and human nature. He therefore succinctly clarifies that human nature is inherited, culture is learnt, but personality is both learnt and inherited. Triandis et al. (2002) in his work on “Cultural Influences on Personality” also reveals that although personality is shaped by both genetic and environmental influences, the most important of the environmental influences is culture. Behaviour they go on to explain is not only a function of both this personality and culture but also varies depending on the interaction between the personality and the situation in which one finds him/herself.

According to Schein (2004), employee behaviour in the organization is largely influenced by the culture, defining culture as the “values, beliefs and assumptions that a group of people share”. In simplifying his definition, Schein (2004) defines organizational culture as “what is valued; the dominant leadership styles, the language and symbols, the procedures and routines; the definitions of success that characterizes the organization; the habit of thinking; people’s mental modes; the climate and the group norm” among others. It is these elements, i.e. shared standard operating procedures, unstated assumptions, tools, norms, habits, values etc. (Triandis et al,2002) that are the characteristics of culture.

There are however a number of these cultural elements or characteristics, which when shared, lived and practiced by an organization inure to the benefit of protecting information assets by way of ensuring and advancing “information protecting” behaviour. This is what Dhillon (1997), Lim et al (2009), Von Solms, R. & Von Solms, B.(2004), among other researchers, define as information security culture. Dhillon (1997, see Lim et al (2009)) defines Information security culture as “the totality of behaviour in an organization that contributes to the protection of information of all kinds“

In moving forward with the research, we made a theoretical proposition based on the many literature we had reviewed and came out with a number of characteristics that we believed when part of the culture of an organization can positively influence the behaviour of employees and lead to achieving success with information security policies. These characteristics include the Management style adopted by the organization: their decision making processes i.e. being inclusive, they “walking the talk”, understanding and involvement in security discussions and implementations etc. It also concerns, Trust & Responsibility: Employees sense of ownership in security issues and the trust with which employees are assigned roles. There is also Bureaucracy & Dependencies: which focuses on organizational structures and the contrast between process-oriented and results-oriented, and the existence, use and dependence on power structures (e.g. influential personnel) in the organization. Motivation discusses ways to incentivize staff either by use of positive (rewards) or negative (sanctions) influences. Budgeting & Funding: is fundamental to any undertaking as it is what is used to acquire all resources during the enforcement and monitoring of security policy implementation. The importance of security awareness training and education is in its ability to continually keep the contents and requirements of the policy fresh in the minds of the employees. The characteristics; Participation & Cooperation, has more to do
with enabling the different viewpoints of the various organization members (employees) and these viewpoints been brought to bear in the decision making process. Commitment reflects the employee’s innate desire and willingness (ideally, because of the values he/she shared with the organization) to work towards meeting the organization’s goals. Communication as revealed by Ruighaver et al. (2007) is centered towards implementing systems that allow information to be shared equally among all relevant members of the organization and among the characteristic of Supervision, Co-ordination & Control is the call for a champion to lead and direct the policy implementation and enforcement.

The above characteristics we have identified as pertinent cultural traits that will ensure that security policy is implemented successfully. Note that these characteristics are not necessarily attributes of employees but that of the organization as a whole single entity. These literature-deduced characteristics were verified in the case organization, UNICEF Ghana by way of a theory-testing approach and were found to largely exist, among other characteristics. The extent to which these characteristics exist in the organization reflects the extent to which the organizational culture influences employees and therefore gives an idea of the extent to which security policies will be successfully implemented. This study however does not delve into estimating the extent to which the characteristics exist. It uses the data collection as indicators for the existence of the characteristic.

One must also understand the entire chain that leads to achieving policy success. As mentioned by Al-Awadi et al. (2007), the aim of information security policy is to change (or better still influence) the habit of employees in the organization so they acquire “information protecting” behavior. In addition to other change agents, the organization’s culture is identified as a powerful latent resource that can be used as a vehicle to effect this behavioral change. Once the organization’s culture is used to effect this behavioral change, one can arrive at the conclusion that the policy will be successfully implemented, since they both have the same goal. The challenge however, lies in identifying what the appropriate organizational culture is and how its constituent cultural characteristics can be adopt or adapt in order to achieve the behavioral change required. Luckily, reviewing extant research reveals to a large extent the right cultural traits that organizations must possess in order to be “information protecting”- which is the ultimate goal of the information security policies.

As explained by Paudel (2009), policy implementation involves those actions by individuals or groups that are directed at the achievement of objectives set forth in the policy. This is supported by Caravan’s (2003) assertion that policy can only be enforced by means of implementation. By this, an information security policy will have been successfully implemented if its contents have been effected and employees of the organization are acting, thinking and behaving according to the policy’s intent.

The main research question is to identify the role that organizational culture has in the successful implementation of information security policies? To answer this, we looked at each of the embedded questions: What factors influence a successful information security policy, in what ways does organizational culture influence information security policy? and what characteristics define this organizational culture?

The first embedded research question is answered mainly from reviewing extant literature. It looks at the research problem from the perspective of information security policies and the challenges it faces in its successful implementation. Adopting this question ensures that the challenges revealed go beyond identifying just organizational culture as an influential factor. This will first help broaden the understanding of the stakeholders concerning the entirety of challenges facing IS policy implementation and position them for their future assigned roles/responsibilities accordingly. Through the review of different literature from different branches of knowledge, we explored the exact relationship between organizational culture and information security policy. The second question is answered by identifying what the exact relationship between organizational culture and IS policy is. An
exploratory process is pursued leading to the development of a theoretical proposition from extant literature. The third embedded question is answered by using the theoretical proposition derived from extant literature as a guide to collect empirical data in a case organization to explore and firm up (or otherwise) the characteristics defined in the proposition. The theoretical proposition that is developed and tested emanates as a set of characteristics that is revealed to organizations to adopt. The characteristics can then further be investigated by other researcher to find easier ways of integrating them into organizations.

The first embedded question is answered looking at a number of contributions of various researchers. In their discussion of the Information security policy process, Knapp et al (2009) discuss IS policy influencers from the perspective of internal and external influences. They discuss the external influences including economic sector, technology advances, industry standards, legal and regulatory requirements and external threats. Their Internal influences include senior management support, business objectives, technology architecture and internal threats and organization culture and it is this last internal influence that provides us the nexus and a starting basis for our research.

Talbot & Woodward (2009) also identify a number of issues with IS policies including a culture of ignorance, minimal policy awareness, ad-hoc updating and a lack of a policy framework. They also identify a lack of compliance and non-compliance reporting as some of critical issues affecting policy success.

In discussing the overarching Information Security implementation (of which information security policy implementation is a first major step), Al-Awadi et al (2007) identify Organization Mission, Budget, Management Support, Awareness & Training and IS policy enforcement & adaptation as a critical success factor.

Whitman & Mattord (2009) discuss the influential factors from the context of a project implementation plan for information security. They mention that the relevant points that need to be attended to include, the time & schedule, assignment of job roles and staffing, the financial and budgetary considerations, task dependencies and training, indoctrination & supervision. Rosenbaum (1986, see Dalton et al 2007) discloses that challenges to policy implementation include lack of resources, inexperienced personnel, and insufficient training. Whilst Durlak and DuPre (2008, see Wandersman et al 2005) see the challenges emanating from a lack of quality adaptation with the original policy plan.

According to the British Standards Institute, BSI (1999), there are eight critical success factors that organizations must adopt in order to be successful with Information security policy implementation. These include, alignment of security policy objectives with business objectives, clear management commitment, proper distribution and guidance of policy to all employees, provision of adequate training and effective marketing of the policy. It also includes ensuring policy reflects risk assessment & business objectives, a metric system to evaluate performance of the policy and last but not the least an alignment between security implementation and the organization’s own culture.

One will find that, a number of the factors that can influence the successful execution or implementation of an information security policy can somehow be traced to or fit into the culture of the organization. This is because the culture is what defines how the organization behaves and acts i.e. whether it will or has the practice of evaluation the performance of policies in general, providing guidance & training on policies, allocating funds for information security programmes, properly assigning tasks & job roles, involving relevant stakeholders in the policy process, aligning all activities to the organization’s objectives or receiving senior management support for policy related activities. This tells us that, it is this organizational culture that largely influences whether an information security policy will succeeds or not.
A number of researchers (Canavan, 2003; Doherty & Fulford, 2005; Hone & Eloff, 2002; Salter et al. 1998; Madigan et al. 2004; Tryfonas et al. 2001; and Dhillon, 1999, see Al-Awadi et al. 2007) mention the need for information security policies to fit with organizational culture in order to be effective and secure the organization’s assets properly. Verton (2000) Nosworthy (2000), Borck(2000) (See Maynard et al, 2002) also attest to the fact that a strong organizational culture has a strong influence on Organizational security and it may in more ways hinder any plans to effect appropriate changes in business processes.

Organizational culture influences information security by way of the characteristics that define it. As explained by Schein (2004), this culture is defined by way of three main characteristics that is Artifacts: the visible structures and processes, Espoused Values: the strategies, goals & philosophies and Underlining Assumptions: the taken-for-granted beliefs, feelings, thoughts – which are the ultimate source of values. Hofstede (1990) similarly chooses to explain this culture in terms of values and practices (symbols, heroes and rituals). The relationship between organizational culture and information security policy therefore lies in the ability of the culture to define appropriate characteristics that will prescribe and dictate the behaviour and actions that employees should live by in order to protect the organization’s information assets.

Reviewing extant literature, we came up with ten cultural characteristics to defined what we believe will lead to the successful implementation of information security policies. They are the Management style, Trust & Responsibility, Bureaucracy & dependency, Motivation, Budgeting & Funding, Awareness, Education and Training, participation & Cooperation, Commitment, Communication and Supervision, Co-ordination & Control. These organizational cultural characteristics was used as an assessment guide in a case organization, UNICEF, but more findings were revealed. The additional findings identified after empirical studies were carried out include integrity, ethics, language heroes, and the use of guidelines. The “Language” finding may however be subsumed under the Communication characteristics in that, when communication is done discreetly and only understood by the organization’s members it helps in guarding against inadvertent revelation of information leading to confidentiality, a major objective of information security. The “Guidelines” finding may also be subsumed under the Awareness, Training & Education characteristics, in that the use of guidelines may be seen as a tool in order to meet the objectives of Training and Awareness. “Heroes” may also been seen as a personification of the Management style characteristic. This leaves the findings Ethics and Integrity.

Ethics is seen more as a standardized prescription of moral rules of the organization that members should live by i.e. what is right and what is wrong. This is difficult to contain it under any of the deduced characteristics and should therefore stand as an additional characteristic that should be lived by the organization and its members. It is an overwhelming characteristic that one is tempted to say, can single-handedly (when adapted will) ensure behaviour that will lead to successful information protection.

Integrity is somehow linked to Ethics but is more of a personal code of conduct that an employee must have for him or herself. Ethics is about following the rules whilst integrity is about doing the right thing regardless of the existence of rules. Integrity is therefore being espoused here as a characteristics that the organization’s members must have and it is incumbent on the organization to find ways to ensure that is members possess this characteristic.

In winding up, we will say that success can be achieved with the execution or implementation of IS policies if the cultural characteristics that have been discussed above are adopted or adapted into the culture of an organization. The difficultly however is to find ways in which these cultural characteristics, that may be alien to an organization can be successfully integrated the organization’s culture to achieve...
the objective of information protection. It is our hope that other researchers will follow up where we are leaving off and finds ways to achieve this.

7.2 Conclusion

The role of organizational culture in achieving success of information security implementation is indispensable. In achieving information security through the successful implementation of policies, the role of the culture of the organization has a direct effect. The beliefs, values, practices etc. of the organization visibly reflect in the behaviour of employees and this also guides their corresponding actions towards adhering to information security policies. The human factor in information security policy implementation (which is still a major issue in information security) remains a major and critical issue to be considered in addressing information security challenges in most organizations.

Our study has revealed that UNICEF Ghana, which is a case of an organization that is succeeding with policy implementation, possesses and is highly characterized by the cultural traits that we deduced as required for the successful implementation of security policy. After going through the study, we are tempted to conclude that the panacea to security policy implementation is not to preach it (as is done by developing and just distributing to all employees to read and acquaint themselves with) but to practice it (i.e. living it in a day to day manner) as part of the organization’s culture. To really establish this assertion, further research has to be carried out in the form of case study experiments by other investigators, following the same approach we have used with the hope that the same conclusions will be arrived at. As explained by Yin (2009), in order to bring reliability to the results of this research, there is a need for the same procedures to be followed to replicate the results.

Kay (2002) tells us that improving security necessarily involves changing beliefs, attitudes, and behaviour, both of individuals and of groups. To do this, we have taken a first step through this research to investigate what we believe are the particular cultural beliefs, attitudes and behaviours of individuals and groups that require changing, in order to improve upon policy and security implementation. We set out to investigate ten cultural characteristics that we deduced from extant literature and have found that by and large, most of them add to improving implementation success with information security policy and information security in general, although data we have collected has not necessarily shown a strong culture of awareness, education and training as influencing the implementation. Perhaps this empirical revelation is supported by Al-Awadi et al. (2007) who also admit that currently there is no clear understanding of the effectiveness of training and awareness programs with the implementation of information security, although it remains a tool in our arsenal with the hope that it will do some good. Whilst collecting empirical data in the case organization however, we also narrowed down on two other characteristics that are worth looking into in the future, these are integrity and ethics. These two characteristics were found to be very explicit and strong in UNICEF environment. The rationalization for these two traits perhaps emanates from the fact that UNICEF is funded by contributions of governments and private organizations and there is a need to show to them and the outside world that things are done in an accountable and transparent manner, but then again, all organizations with a need to successfully implement information security policies are also “held ransom” by their stakeholders to this same requirements. In actuality, these characteristics have already been discussed in research by Dhillon & Backhouse (2000) in their work on “Information Systems Security Management in the new Millennium” where they discuss the RITE principles. The RITE is an acronym for Responsibility, Integrity, Trust and Ethicality and they suggest organizations consider...
them as the first steps in securing their information assets in the future. We have already shared consensus with two of the principles: Responsibility and Trust and also Integrity and Ethicality is what we have identified in the case organization that needs further research into.

Going through previous research, we have consistently come across information security culture being referred to as some separate artifact or program which has to be introduced and practised differently without taking cognisance of the organizational culture that is already in existence. It is of our view that the challenge of this approach is that, the outright introduction of a new culture is something that will be very difficult to achieve. Should this be the case, every department in the organization with an agenda to implement some program will come forth with its own requirements (which comes with resources and possibly culture) and this will overwhelm the organization. The idea is to take advantage of what already exists by adapting the security requirements to the existing organizational culture. Any agenda that does not adopt this adaptation approach is likely to face resistance challenges among others.

7.3 Further Research

We have a number of research ideas that we also believe are worth looking into in future studies. The first one is on how to adapt and adopt the identified cultural characteristics into organizations. This is because the real benefits of this research will be achieved if suitable ways are identified to integrate the identified culture characteristics into organizations so they can profit from low-cost security policy implementation. This adoption process may also involve an examination of the current culture in the organisation to highlight areas that require greatest attention for change. This means for organizations that have the prescribed cultural traits, how to distinguish between those that have stronger and weaker culture (Chatman et al. 2012).

Future research will also want to look into the possibility of overlaying the identified organizational cultural traits against the national culture of a particular country. This will allow for example multinational organizations to know the challenges in the organizational culture that are likely to exist in a particular country and therefore commit more resources to changing or managing those deficient cultures traits to improve upon IS policy implementation success. For example a country may by their culture be challenged with communication and therefore an organization looking to come in and setup its business will then have to critically look at improving this cultural trait if it intends to successfully implement IS policies in its business in that country.

7.3.1 Why Implementation and not compliance

The essence of implementation is to execute the contents of a security policy but the idea behind compliance is to force adherence to rules, which is not what we hoped to achieve here. This research hoped to turn us away from the use of compliance in the strictest sense i.e. forcing strict mechanistic employee behaviour. In the everyday situation where we live out our lives as part of our culture, compliance is only mentioned as a deterrent when a member tries to stray out of the lawful/ethical boundaries of the society. Many have therefore come to understand compliance as a negative undesirable thing. It will be more subtle and more easily be imbibed by our unconscious mind if we live out information security policies as part of the culture of the organization and not as part of some mandatory requirement for which there are strict consequences if we should flout them.
7.4 Steps to Achieving Success with policy Implementation

We are tempted to propose a cultural guide to achieve success with information security policy implementation. The stages we see involved in living out appropriate organizational culture that will bring success to security policy implementation and ultimately information security is to

1. Identify the appropriate organizational values that will enhance and stimulate positive human behaviour towards policy implementation. *(Which we have done in this research)*
2. Pursue an organizational culture change program through the adaption and adoption of those values that will improve upon policy implementation success.

The change program involves identifying and recognizing those values that are already strong in the organization and working on strengthening the values that are identified to be weak in the organization. From extant literature and discussion by seasoned researchers in organizational change, this can be mainly achieved through the organizations leadership when they start practicing i.e. living out those culture practices themselves for other employees to follow.

This is our definition of a framework that will allow for increased success rate of policy implementation in organizations.

7.5 Limitations

We have been limited mainly by the time required to complete the project. More time will have allowed us to collect a cultural data at a deeper level to further buttress our proposition of the cultural traits. This notwithstanding, we believe we have collect adequate data to validate our theoretical proposition. As explained we have only taken baby steps towards finding a cost-effective solution to achieving success with the implementation of information security, the rest rests in the boson of future research to take up from where we have ended.
8 References

Adamson, P., Bellamy, C., Gautam, K., Jolly, R., Nyi, N., Racelis, M., Reid, R., Rohde, J. (). Jim Grant UNICEF Visionary


Chatman, J., Caldwell, D.F., O'Reilly, C.A. III, & Doerr, B. (2012) Organizational Culture and Performance in High-Technology Firms ; The effects of Culture Content and Strength


Hermans, L. M .(2010).Ten reasons not to monitor policy implementation and what this means to evaluations. 9th European Evaluation Society International Conference, October 6-8, 2010, Prague.


ISACA (2012). COBIT 5 for information security


Lok, P & Crawford, J. (1999). The Relationship between Commitment and Organizational Culture, Subculture, Leadership Style and Job Satisfaction in Organizational Change and Development


McNamara, Carter, PhD. General Guidelines for Conducting Interviews, Minnesota, 1999


Ofori, D. F., & Sokro E. Examining the impact of organizational values on corporate


UNICEF ICT Policies.

UNICEF Staff Rules and Regulations,


UN Code of Ethics.

Standards of Conduct for International Civil Servants.
Appendix A: Interview Guide

Before beginning the interview session we provided a short explanation of the reason for the interview and also discussed some definitions with participants, among some of the explanations are

1. Information security – The protection of information from unauthorized disclosure, modification, damage, destruction and theft, whilst making the right information available when required in a timely manner
2. Information Security Policy – Rules and regulations laid down to ensure the successful implementation of security conditions
3. Culture – Is the way things are done here, the norms, the beliefs, the practices and the principles that the organization believes in and lives by.

Management Style

1. Is management proactive when dealing with policies, initiatives, and projects?
2. Does management usually exercise oversight responsibilities over the implementation of projects, initiatives and policies?
3. Do you think management adequately gets involved in the implementation of policies, projects and initiatives?
4. Does management usually delegate the supervision of implementation of projects, initiatives or policies to other supervisees?
5. Does management frequently demand progress reports or feedbacks on implementation of projects, initiatives and policies?
6. Is management quick to review issues arising from progress report on projects and initiatives?
7. Does management fully support and offer assistance to people in charge of projects and initiatives including policy implementation?
8. Does management seek your input in the implementation of policies, projects or initiatives?
9. Is there a ‘closed group’ of persons responsible for making decisions in your organizations, and does the group take input on decision making from other employees?

Trust and Responsibility

1. Do you collectively take responsibility for the success of new projects, initiatives and policies within the organization?
2. Do you trust managers to take initiatives, implement policies and make decisions in the broader interest of employees within the organization?
3. Do you openly accept responsibilities for your actions whether the result of your actions were good or bad?
4. Do you have a full understanding of your job role in the organization?
5. Have you developed work practices or techniques to perform your job function?
6. Does this technique or practice fall in line with the organization's rules and regulations?
7. Do you really feel as if this organization's problems are your own?
8. Do you have any responsibility in the formulation and implementation of projects, initiatives and policies?

Bureaucracy and Dependencies

1. Does the organization have standardized procedures in place for dealing with daily routine activities?
2. Do these procedures enhance or impede the smooth completion of tasks?
3. Can employees take actions which they deem right without necessarily following some laid down procedures?
4. Does the completion of your work depend a lot on others completing theirs?
5. Are you commended for completing a task even if you cut corners to complete them?
6. Do you regard you organization to be process or results oriented?
7. Do you understand how your job contributes to the organization’s goals and objectives?

**Motivation**

1. Are you appropriately rewarded (financially, recognition, promotions, etc.) when you partake in the implementation of a project, initiative or policy?
2. Are you inspired by the reward received a fellow employee to do your best and succeed in all your work endeavors?
3. Are you well-resourced to perform your duties in the organization?
4. Are your suggestions or views considered in rolling out projects, initiatives or projects?
5. Do you feel you are well motivated to continue working with your organization?
6. Do you have any special reasons for working with your organization?
7. Do you gain any returns such as promotion, praises, recommendation etc. after you receive a good performance appraisal?
8. Are you pressured or encouraged by the performance of your work colleagues to work harder at your job?
9. Do you feel pressured or encouraged by your work environment to achieve more at your work?

**Budget and Funding**

1. Generally, is there allocation of funds for the implementation of policies in the organization?
2. Does the organization provide adequate funding for all projects, initiatives such as policy implementation?
3. Does the organization live within its means, i.e. is spending based on its annual budget?
4. Does the organization give higher priority to particular projects and initiatives such as policy implementation?
5. Does the organization have ways to monitor spending on all projects, initiatives, such as policy implementation?
6. Is management in the habit of diverting funds for other projects to allocate to high priority projects such as policy implementation?
7. Is there a strict funding mechanism for projects and initiatives in your organization?

**Awareness, Education and Training**

1. Are you well informed on the implementation of projects, initiatives such as that related to policies, in the organization?
2. Do you receive periodic updates and information related to projects, initiatives in the organization?
3. Have you received any training or education with regards to the implementation of projects and initiatives such as policy?
4. Did you receive any orientation on the organization’s policies when you first joined the organization?
5. Are you regularly obliged by management to attend awareness, education and training sessions?
6. Have you recently attended a training or workshop on the implementation of projects or initiatives?
7. Do you know whether funds are budgeted for awareness, education or trainings related to the implementation of a project or initiative?
8. During training workshops are you made aware of the rationale (and or advantages/disadvantages) behind the project or initiative?
9. Are awareness trainings carried out together for all employees or for different categories of staff?

**Participation and Cooperation**

1. Are people encouraged to work in groups or teams on implementation projects or initiatives?
2. Are you invited to participate in meetings and activities related to implementation of projects, initiatives such as that related to policies?
3. Are people cooperative when it comes to projects, initiatives, and policies implementation?
4. Does the organization’s environment make you comfortable to freely contribute during meetings and discussions?
5. Does your organization support team or group works?
6. Are there periodic meeting between different sections and units in your organizations?
7. Are you obliged to attend meetings in your department or organization?
8. Are you part of a regular meeting in your sections or units?
9. Do teams working on the implementation of projects or initiatives usually comprised of members from different sections of units?
10. Are your viewpoints considered during meetings to arrive at a consensus on decision making?

**Commitment**

1. Are you willing to put in a great deal of extra effort to help the organization succeed in implementation of projects or initiatives?
2. Do you see yourself as part of the organization?
3. Are your own values similar to that of the organization?
4. Do you feel encouraged to work towards achieving the organization’s objectives?
5. Do you have any positive feeling towards working for the organization?
6. Do you think you will still continue to have this positive feeling when you live this organization?

**Communication**

1. Do you easily receive the information you need in order to do your job in the most effective and efficient manner?
2. Do you know where you can get the information you need in order to do my job well?
3. Do you receive information about anything that might affect your job in a timely manner? Is the communication that you receive clear and understandable?
4. Are you satisfied with the frequency and level of communication you have with your immediate supervisor?
5. Do you feel you communicate frequently and adequately with your work colleagues?
6. Do you feel there is effective and adequate communication with management?
7. Do you feel there is adequate communication during meetings?
8. Do you feel information is communicated freely in your organization?
9. When you first joined the organization, did you feel you warmly received?
Supervision, Coordination and Control

1. Is there a designated person who leads the implementation of projects and initiatives?
2. Is the designated person usually a member of management or senior person in the organization?
3. Are there clearly-spelt out disciplinary measures to be meted out when employees go contrary to rules and regulations?
4. Are there punitive measures for punctuality and timeliness in your organization?
5. Does your organization have a concrete follow-up plan for the implementation of projects and initiatives?
6. Does your supervisor interact with you frequently for supervision purposes?
7. Do you think management or the organization speedily acts on the implementation of projects and initiatives?
8. Generally do you feel the organization has a centralized or a decentralized decision making process?
9. Do you feel the hierarchy between you and top management is too high?
10. Does the organizational structure affect the response time to decision making requests on the implementation of projects and initiatives?

General questions

1. Name some cultural characteristics that you think are important in this organization
2. Do you think the organization acts on these characteristics that you deem important?
3. Do you have any particular person that inspires you to work for UNICEF?
## Appendix B: Extracts of UNICEF Competency Framework Definitions and Behavioral Indicators

### Core Values

<table>
<thead>
<tr>
<th>Core Competency</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diversity and Inclusion</td>
<td>Treats all people with dignity and respect; shows respect and sensitivity towards gender, cultural and religious differences; challenges prejudice, biases and intolerance in the workplace; encourages diversity wherever possible.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Maintains high ethical standards; takes clear ethical stands; keeps promises; immediately addresses untrustworthy or dishonest behavior; resists pressure in decision-making from internal and external sources; does not abuse power or authority.</td>
</tr>
<tr>
<td>Commitment</td>
<td>Demonstrates commitment to UNICEF’s mission and to the wider UN system; demonstrates the values of UNICEF in daily activities and behaviors; seeks out new challenges, assignments and responsibilities; promotes UNICEF’s cause.</td>
</tr>
</tbody>
</table>

### Competencies

#### Core Competencies

<table>
<thead>
<tr>
<th>Core Competency</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication</td>
<td>Speaks fluently; expresses opinions, information and key points of an argument clearly; presents information with skill and confidence; responds quickly to the needs of an audience and to their reactions and feedback; projects credibility; structures information to meet the needs and understanding of the intended audience; presents information in a well-structured and logical way.</td>
</tr>
<tr>
<td>Working with People</td>
<td>Shows respect for the views and contributions of other team members; shows empathy; listens, supports and cares for others; consults others and shares information and expertise with them; builds team spirit and reconciles conflict; adapts to the team and fits in well.</td>
</tr>
<tr>
<td>Drive for Results</td>
<td>Sets high standards for quality of work; monitors and maintains quality of work; works in a systematic, methodical and orderly way; consistently achieves project goals; focuses on the needs and satisfaction of internal and external partners; accepts and tackles demanding goals with enthusiasm.</td>
</tr>
</tbody>
</table>

### Functional Competencies
<table>
<thead>
<tr>
<th>Competency</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deciding and Initiating</td>
<td>Takes responsibility for actions, projects and people; takes initiative and works under own direction; initiates and generates activity and introduces changes into work processes; makes quick, clear decisions which may include tough choices or considered risks.</td>
</tr>
<tr>
<td>Leading and Supervising</td>
<td>Provides others with a clear direction; motivates and empowers others; recruits staff of a high caliber; provides staff with development opportunities and coaching; sets appropriate standards of behavior.</td>
</tr>
<tr>
<td>Relating and Networking</td>
<td>Easily establishes good relationships with external partners and staff, builds wide and effective networks within UNICEF, within the wider UN system and with external parties; relates well to people at all levels; manages conflict; uses humor appropriately to enhance relationships with others.</td>
</tr>
<tr>
<td>Persuading and Influencing</td>
<td>Gains agreement and commitment from others by persuading, convincing and negotiating; makes effective use of political processes to influence and persuade others inside and outside UNICEF; promotes ideas on behalf of oneself or others; makes a strong personal impact on others; takes care to manage one’s impression on others.</td>
</tr>
<tr>
<td>Applying Technical Expertise</td>
<td>Applies specialist and detailed technical expertise; develops job knowledge and expertise (theoretical and practical) through continual professional development; demonstrates an understanding of different organizational departments and functions.</td>
</tr>
<tr>
<td>Analyzing</td>
<td>Analyzes numerical data and all other sources of information, to break them into component parts, patterns and relationships; probes for further information or greater understanding of a problem; makes rational judgments from the available information and analysis; demonstrates an understanding of how one issue may be a part of a much larger system.</td>
</tr>
<tr>
<td>Learning and Researching</td>
<td>Rapidly learns new tasks and commits information to memory quickly; demonstrates an immediate understanding of newly presented information; gathers comprehensive information to support decision making.</td>
</tr>
<tr>
<td>Creating and Innovating</td>
<td>Produces new ideas, approaches, or insights; creates innovative ways of designing projects or outputs in own work area; produces a range of solutions to problems.</td>
</tr>
<tr>
<td>Formulating Strategies and Concepts</td>
<td>Works strategically to realize UNICEF's goals; sets and develops strategies; identifies and develops positive and compelling visions of the organization’s future potential; takes account of a wide range of issues across, and related to, UNICEF.</td>
</tr>
<tr>
<td>Planning and Organizing</td>
<td>Sets clearly defined objectives; plans activities and projects well in advance and takes account of possible changing circumstances; identifies and organizes resources needed to accomplish tasks; manages time effectively; monitors performance against deadlines and milestones.</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Following Instructions and Procedures</td>
<td>Does not unnecessarily challenge authority; follows procedures and policies; keeps to schedules; complies with legal obligations and safety requirements of the role.</td>
</tr>
<tr>
<td>Adapting and Responding to Change</td>
<td>Adapts to changing circumstances including emergencies and other crises; tolerates ambiguity; accepts new ideas and change initiatives; adapts interpersonal style to suit different people and situations; shows an interest in new experiences.</td>
</tr>
<tr>
<td>Coping with Pressure and Setbacks</td>
<td>Maintains a positive outlook at work; works productively in a pressurized environment and in crisis situations; keeps emotions under control during difficult situations; handles criticism well and learns from it; balances the demands of a work life and a personal life.</td>
</tr>
<tr>
<td>Entrepreneurial Thinking</td>
<td>Keeps up to date with trends in own work area; identifies opportunities for advancing UNICEF's mission; maintains awareness of developments in the organizational structure and politics; demonstrates financial awareness and a concern for cost-effectiveness.</td>
</tr>
</tbody>
</table>

**Knowledge and Skills**

Taxonomy as per job family/level (see GJP)