A Study in an IT Company
Abstract

There is a great concern when it comes to the investigation of the parameters that affect the formulation of an information security management strategy in an organization. Amongst others, information security awareness is of great interest, mainly because it links the implementation of the information security policies to the consciousness and the psychology of the employees of an organization. State it otherwise, the information security awareness positively beholds the role of a bridge so as to help the IS managers to evaluate the level that the critical information of the organization are secured, and it offers to IS managers opportunities to develop suitable training programs and information security policies for all the employees of an organization. In the current thesis, we focused on the investigation of the factors that influence the behavior of the employees in order to accept any information security policy of the organization and to adopt information security awareness.

The psychology of security and technology (POST™) framework (Layton, 2005) together with a PEST (Political, Economic, Social, Technology) analysis guide the investigation and offer the theoretical background for the conduction of a study in an IT Company. A qualitative research has been conducted and semi-structured interviews helped for the collection of the desired data. Also a thematic analysis and the use of a generic approach (Lichtman, 2013) helped for the analysis of the data. The final results gave the ability to identify in practice the employees’ information security awareness adoption level, to link the measurement findings to the development of an information security management strategy and to refine the POST™ framework for its greater advance.

Keywords

Information security awareness, information security policies, compliance, psychology, security, measurement, information security management strategies, information security training programs, POST™ framework, PEST analysis.
Acknowledgements

I would like to thank:

Linnaeus University of Sweden which gave me the opportunity to be a student to the Master program of Information Systems.

Prof. Christina Mörtberg for her guidance and her valuable feedback for the thesis.

My supervisor Dr. Miranda Kajtazi for her guidance and help to complete the thesis.

My three daughters Efrosini, Dimitra and Christina, which gave me the strength to continue to be in this Master program and finish it. I love you girls…..and I’ll always do.

My father, my brother, and my sisters for their love and support.

My friends for their understanding.

Finally I dedicate all my Master Thesis in memory of my mother, Efrosini Spandonidou, which I will always remember with nostalgia and love…
# Table of Contents

Abstract .......................................................................................................................... ii

Keywords ....................................................................................................................... ii

Acknowledgements ....................................................................................................... iv

Table of Contents .......................................................................................................... 6

List of Figures ................................................................................................................. 8

List of Tables ................................................................................................................... 8

List of Abbreviations and Terms ..................................................................................... 8

Chapter 1: Introduction ................................................................................................. 10
  1.1 Research Motivation ............................................................................................... 10
  1.2 Topic Justification .................................................................................................. 11
  1.3 Aim and Research Questions .................................................................................. 13
    1.3.1 Research Questions ......................................................................................... 13
  1.4 Thesis Scope and Limitations ................................................................................. 15
  1.5 Thesis Structure .................................................................................................... 15

Chapter 2: Literature Review ....................................................................................... 18
  2.1 Previous Studies that have addressed the Problem ................................................. 18
  2.2 Deficiencies in the Previous Studies ..................................................................... 20
  2.3 POST™ Framework ............................................................................................... 23
    2.3.1 Motivation ......................................................................................................... 28
    2.3.2 Attitude ............................................................................................................. 31
    2.3.3 Beliefs .............................................................................................................. 32
    2.3.4 Personality ....................................................................................................... 32
    2.3.5 Morals .............................................................................................................. 34
    2.3.6 Ethics ............................................................................................................... 36
  2.4 PEST Analysis ....................................................................................................... 37
  2.5 Use of the Literature ............................................................................................... 40

Chapter 3: Methodology ............................................................................................... 42
  3.1 Philosophical Worldview ....................................................................................... 42
  3.2 Research Setting ..................................................................................................... 44
  3.3 Research Strategy ................................................................................................... 45
  3.4 Data Collection ..................................................................................................... 48
List of Figures

1.1 Thesis structure .................................................................................................................. 16
2.1 POST™ framework ............................................................................................................. 25
2.2 Human behavior ................................................................................................................ 26
2.3 The most common categories of OCB ............................................................................... 28
2.4 Theories of motivation ....................................................................................................... 29
2.5 Personality’s types and approaches .................................................................................. 34
2.6 Representative theories for Morals .................................................................................. 35
2.7 PEST Analysis .................................................................................................................. 39
3.1 Strategically selected axes for the operations of the IT company ..................................... 45
3.2 Type of the research .......................................................................................................... 46
3.3 Research strategy ............................................................................................................. 48
3.4 Data analysis circles ......................................................................................................... 51
4.1 Steps of the ISMS ............................................................................................................. 75
4.2 POST™ framework refinement ...................................................................................... 81

List of Tables

4.1 Themes of the analysis ...................................................................................................... 58
4.2 Measurement Findings ..................................................................................................... 68
4.3 PEST analysis .................................................................................................................. 74

List of Abbreviations and Terms

Actor Network Theory ........................................................................................................... ANT
General Deterrence Theory ..................................................................................................... GDT
Human Aspects of Information Security Questionnaire ..................................................... HAIS-Q
Information Security ............................................................................................................ IS
Information Security Awareness ............................................................................................ ISA
Information Security Awareness Program( s) ........................................................................ ISAPM(s)
Information Security Management Strategy(ies) ................................................................. ISMS(s)
Information Security Policies ............................................................................................... ISP
Information Security Training Program(s) ........................................................................... ISTP(s)
Information Technology ...................................................................................................... IT
Organizational Citizenship Behavior ..................................................................................... OCB
Political, Economic, Social, Technology ................................................................................ PEST
Psychology of Security and Technology ................................................................................ POST™
Qualitative Data Analysis Software( s) .................................................................................. QDAS(s)
Global Entrepreneurship Monitor .......................................................................................... GEM
Small and Medium-sized Enterprise(s) ................................................................................ SME(s)
Small Business Act ............................................................................................................... SBA
Value Added Tax .................................................................................................................... VAT
European Union .................................................................................................................... EU
Information Security Retrieval and Awareness ..................................................................... ISRA
Chapter 1: Introduction

Chapter 1 begins with an introduction to the research problem and a discussion about its importance to the information security field. The chapter continues with an analysis of the aim and objectives of the thesis and then with a presentation of the research questions. The last two subsections contain the scope and limitations, and the structure of the thesis.

1.1 Research Motivation

Previous studies show that many researchers tend to focus on the value of information security awareness (ISA), primarily for the establishment of an information security policy (ISP), which is followed by the development of an information security management strategy (ISMS) in an organization (Siponen 2000, Puhakainen & Siponen 2010, D’Arcy et al. 2009). Bulgurcu, et al. (2010, p.532) argue that “information security awareness is an employee’s general knowledge about information security and his cognizance of the ISP of his organization”. Also the authors state that ISA has two dimensions, the general ISA (i.e. when an employee understands all the related issues that have to do with information security and its bifurcations) and the ISP awareness (i.e. the awareness that is related with the employees’ willing to respect the organizational ISP and to understand its requirements and its purposes). Although many organizations have built their ISMS according to the map directions of the ISO/IEC 27001 (ISO, 2005); (Tsohou et al., 2012) or ISO/IEC 27002 (Kajtazi, 2013), a lack of knowledge relating the factors that guide the formulation of an ISA climate to the employees and the columns that hold the root definitions for the evaluation of the existing level of employees’ awareness in the organization is revealed. In addition, many researches try to identify the means or tools to measure ISA, the reasons for compliance or not compliance with ISP, and much literature concerns the construction of ISP and the definition of tactics for the imposition of their norms to the employees. But the problem is that limited literature about ISA is based on the psychology of the end users and on the discovering of “why” the employees choose to respect or not the organizational ISP (Layton, 2005).

Siponen (2000) argues that the end users have to accept the meaning of the adoption of any ISP and they have to internalize this meaning before they accept it. The internalization of the meaning of ISA is very critical for Layton (2005), as this is the key for the compliance with any ISP, and this internalization depends on psychology of the end users. There is a need for investigation of new measurement tactics that will be based on the psychology of the end users and these tactics have to be built on the context of information security (IS) area so as to correlate the new knowledge with all the previous knowledge on the field. The examination of the relation between the psychology of the end users and their ISA adoption level can bring light into the identification of acceptable ISMSs. Information security awareness is all those factors that affect the compliance of the employees of an organization with its ISP and although many studies afforded to illustrate the high influence of deterrence theory, ethics, organization culture, training programs and alike to ISA, there is a lack of knowledge relating all of the psychological factors that contribute to the desire of someone to accept an ISP (Layton, 2005). The psychology of the employees is the key for the creation of measurement tactics, in order to define the adoption level of information security awareness in an organization and after that the
construction of information security policies that suit with the culture of the organization (Kajzer et al, 2014).

This thesis studies the importance and the benefits of ISA in an organization and examines the manners how ISA can be controlled, measured and further developed to keep a good security climate in an organization. A key issue is the identification of the affection of the behavior of the end users to the development and the implementation of ISA. According to Layton (2005) the six psychological constructs of motivation, attitude, beliefs, personality, morals and ethics influence the behavior of the end users and define their ISA adoption level, thus he developed the psychology of security and technology (POST™) framework so as to help the IS managers of the organizations to “measure” the ISA adoption level of their employees.

Despite that many organizations don’t want to cooperate with the researchers who conduct studies in the IS field (e.g. so as not to reveal their IS tactics, etc…) or choose to accept the cooperation with researchers that conduct quantitative studies in the IS field (Liu, Tanaka and Matsuura, 2008), an information technology (IT) company from the region of West Thrace in Greece agreed to cooperate for the conduction of a qualitative research. The ISA adoption level of the employees of the IT company is measured with the use of POST™ framework, and the extraction of the final results is depended on conducting a thematic analysis of the data together with a PEST (Political, Economic, Social, Technology) analysis (Ward and Peppard, 2002);(Chaffey and Wood, 2005).

According to Wylder (2003) the information security (IS) manager and the information systems manager are responsible to manage the information of an organization. The Author (2003, p.19-20) also states that the duties of an IS manager are: 1) the authentication (i.e. identify users or services that want to have access to the organizational systems or information resources), and 2) authorization (i.e. balance the needs and wants of the end users against the risks and threats to an organization). The outcomes of this study give the ability to further develop the POST™ framework and provide a theoretical background for the IS managers so as to access the adoption level of ISA in their organization and improve it while linking it with to their overall ISMS.

1.2 Topic Justification

Despite of numerous security studies, few tend to focus on the psychology of the employees and understand why they would adopt or not ISA in their organization (Parsons et al, 2014; Maqousi, Balikhina and Mackay, 2013; Kajzer et al, 2014; Kruger and Kearney, 2006; Puhakainen and Siponen, 2010; Eminagaoğlu, Uçar, and Eren, 2009; Maqousi, Balikhina and Mackay, 2013; Bulgurcu et al, 2010; D’Arcy et al, 2009; Johnston and Warkentin, 2010; Kajzer et al, 2014; Myrry et al, 2009; Albrechtsen and Hovden, 2010). Most of the IS studies follow the descriptive approach and treat the ISA issues as an outcome based procedure where the IS managers develop certain ISP and demand from their employees to follow them, and when there is a divergent behavior by the employees then the IS managers develop ISMSs (e.g. ISMSs based on sanctions) in order to make their employees to be compliant with the organizational ISP (Layton, 2005). For the prescriptive approach the focus on IS is given in the behavior of the end users and their internalization of the meaning of the issues and the policies that are related with IS (Siponen, 2000). The
ISA adoption level of the employees is influenced by the psychological constructs that constitute their behavior and these constructs can only be measured in an indirect way (Layton, 2005). In this thesis it is presented the background theory that is related with the psychological constructs that constitute the behavior of the end users, testing them in an IT company. Despite borrowing existing theory, revisions to theory are made in order to contextualize for the purpose of this study, so as to understand in general the reasons of why the employees adopt or not ISA in their organization (based on their behavior), which are the intrinsic and extrinsic factors that influence the internalization of the meaning of IS by the employees, and how can the external political, economical, social and technology factors affect the operations of an organization, its strategies and its employees’ behaviors. The theoretical background that helps for measuring whether ISA plays an important role in increasing compliance in an organization (in this study the focus is on an IT Company) is the POST™ framework adopted from Layton (2005) and the PEST analyses (Ward and Peppard, 2002);(Chaffey and Wood, 2005) that support the arguments and the formulation of the final results. The intention of using POST framework and PEST analysis is to measure in an indirect way (i.e. with the conduction of semi-structured interviews) the ISA adoption level of the employees while examining the relationship between the psychological constructs of the employees’ behaviors and their ISA adoption level, as also the affection of the external political, economical, social and technology factors to the employees behavior and their final decision to be compliant with the company’s ISP. The intention is to discover through a prescriptive approach the reasons of why the employees are aware or not to IS issues and the company’s ISP and it is tried to link the answer of the above question to the development of an ISMS that can help the company to overcome its IS problems (i.e. help the IS managers to develop their ISMS while ensuring that it will be acceptable by the employees of their organization). Layton (2005) stresses that the POST™ framework needs more research in order to become better as a measurement tactic and hence better as theory, meaning that the outcomes from the researches may provide new findings about the affection of the behavior of the end users to adopt ISA and may illustrate new tactics for the measurement of the ISA adoption level in an organization.

So there is a trial for further advance of the framework as: 1) there are proposed ways for the measurement of the ISA adoption level in a company while using the background theory of POST™ framework (i.e. advance as a measurement tactic and improvement of the formulated interview guide for the conduction of the study in the IT company accordingly to the results of the study), and 2) there is an argumentation about the connection of the theories between POST™ framework and PEST analysis and there are statements, that are based on findings after the study in the IT company, about how can the behaviors of the employees affect their ISA adoption level (i.e. advance as theory). More specifically for the advance of POST™ framework it is suggested (after the conduction of a study in the organization) an “infiltration” of the measurement results with PEST analysis so as it can be identified by the IS managers of the organization of which of the factors that contribute to the non-respect of the IS issues and policies are related with the external environment of the organization and how can these factors be removed in order that the employees of the organization can adopt ISA. The infiltration of the measurement results helps also to discover if the employees will change their behavior and adopt ISA when the external environment of the organization will satisfy their “willing”.

12
Another improvement of the framework concerns the employees that adopt ISA and respect the IS issues in general and the ISP of the organization. An infiltration that is suggested for the measurement results is the division of the employees that adopt ISA or not in two categories. The first category includes the employees that don’t adopt ISA and examines the reasons for such behavior, for the construction of ISMSs that will implement ISA in the organization. The second category includes the employees that adopt ISA but have similarities in the psychological constructs of their behavior with the employees that don’t adopt ISA. The purpose of this “filter” of the measurement results is to stress that there is a need for the construction of an ISMS separately for the employees that adopt ISA because the IS managers have to ensure that these employees will continue to be aware of the organizational IS issues and policies with the pass of time. After the construction of ISMSs for the employees that adopt ISA and for those that don’t adopt ISA in the organization, it is born the need for the amalgamation of the two ISMSs into one.

1.3 Aim and Research Questions

It is important that the IS managers of an organization will be in the position to measure the employees’ ISA adoption level, to develop suitable ISMSs (according to the measurement findings), and to ensure that there won’t be a leakage of the organization’s secured information. The behavior of the employees influences the ways they understand the world around them, their emotions and their beliefs. According to Layton (2005) and Siponen (2000) the end users have to internalize the meaning of the ISP and norms so as to accept them. So, the IS managers of the organizations need to take into consideration the influence of the psychology of the employees to their behavior, and in turn, to their ISA adoption level while they develop their ISMS. The aim of this thesis is to identify whether the employees of the IT company adopt or not ISA, why they do or do not adopt it and whether there are similarities between those who adopt and those who do not adopt ISA. Also great focus is given into the exploration of the connection links between the above mentioned findings and the development of an ISMS that will try to ensure that all of the employees of the IT company will adopt ISA.

In order to achieve the aim of the study, the first objective is the development of a measurement tactic for the collection and the analysis of data, based on the use of the background theory. The second objective is the development of a methodology which can be used by the IS managers so as to link the measurement findings to the development of ISMSs. The empirical findings of the research illustrate the areas that need more attention from the scope of the IS managers and the areas that need further investigation and reformulation from the scope of the researchers (i.e. reformulation or expansion of the POST™ framework).

1.3.1 Research Questions

The main research question in this study tackles the identification of the tools and means that can be used by the IS managers so as to ensure that there is ISA in their organizations before they plan their ISMS. Furthermore, the exploration of the following strategic questions guides this study to reach its aim and objectives. The existing literature about the affection of the psychology of the end users to their compliance with information security issues and policies helps to answer the
questions. Both the two questions are theoretically and empirically answered by the conduction of a study in a company, to identify a tactic for the measurement of the ISA adoption level by its employees and to link the measurement findings to the development of ISMS by the IS managers of the company.

**How the ISA adoption level in an organization can be identified?**

There is a variety of measurement tactics that are based on the psychology of the end users and have been used for the identification of the ISA adoption level in an organization. So the above question is answered theoretically by the reference of measurement tactics that try to identify the ISA adoption level in an organization (Parsons et al, 2014; Maqousi, Balikhina & Mackay, 2013; Kajzer et al, 2014; Kruger & Kearney, 2006), and by the further expansion of the theory of POST™ framework as a measurement tactic. The empirically part of the question is fulfilled by the development of a measurement tactic based on POST™ framework and with the construction of questions that try to identify whether the employees of the IT company adopt or do not adopt ISA, why they adopt it or not, and whether there are similarities between those who adopt and those who do not adopt ISA. The questions are used as a map for the conduction of semi-structured interviews where the stakeholders are free to express their opinions and the researcher formulates supplementary questions when needed. The data (that are collected through the interviews with the employees of the IT company) are further analyzed by the use of the background theory and the use of PEST analysis so as to examine the role of the external factors when the employees decide to respect or not the company’s ISP. The outcomes illustrate the areas of the measurement tactic that need further advance and the ways that the measurement tactic can be improved.

**How can the measurement findings be linked to the development of ISMS by the IS managers of an organization?**

The development of ISMS can be very important if the IS managers of an organization understand that their employees have to internalize the meaning of the ISP (Layton, 2005), but it can also be time consuming if the employees won’t accept the importance of ISP. Through the first question it is possible to identify the “why” for respect or not of the organizational ISP and the reasons for the adoption of ISA or not. This is the main key for the answer of the second question, as it is tried to adjust the development of the ISMS of the company to the measurement findings. In other words the answer of the above question is the analysis of the factors that contribute to the non-compliance with the company’s ISP and adoption of a security strategy that tries to remove those factors. The theoretical part of the question is covered by the background theory of the previous question and the reference of different ways that the IS managers can build their ISMSs (e.g. formulation of ISP and training programs, sanctions, etc…). The empirical part is covered through the conduction of the interviews in the IT company and the analysis of data. While conducting the interviews it was tried to be discovered of which ISMSs had been adopted in the IT company until the time of the interview and how did these ISMSs influenced the behavior of the employees so as to adopt ISA or not, and the outcomes of the analysis of data helped to suggest an ISMS that would help the IS manager to achieve an ISA climate in the IT company (i.e. strategies that better suit with the measurement findings of the first question and the employees’ behaviors of the IT company).
1.4 Thesis Scope and Limitations

The thesis scope is to answer the above research questions and produce statements about tactics that can be used by the IS managers in order to increase the ISA adoption level of the employees in their organizations. The research questions are the guide map because on the one hand it can be discovered the factors that affect the behaviors of the employees and their ISA adoption level and on the other hand it can be developed ISMSs that will try to advance an ISA climate in the organization. But before the development of the ISMSs there’s a need for use of an effective measurement tactic which can provide outcomes about the number of the employees that don’t adopt ISA, the number of the employees that adopt ISA, and the number of the employees that adopt ISA but they perform similar characteristics in their behavior with those that don’t adopt ISA. Also the measurement tactic that will be used has to enhance the ability of those that conduct the measurement (e.g. IS managers) to identify the reasons that guide the final decision of the employees to adopt ISA or not. Great focus is given to the examination of the role of the behavior of the employees to their compliance with the IS issues and norms in general. The examination of the relation between the behavior of the employees and their ISA adoption level helps to produce arguments about the ISMSs that can be developed in accordance with the “desires” of the employees.

The existing literature about the influence of the behavior of the end users to their ISA adoption level is tried to be enriched with the conduction of a study in an IT company. The first objective of the study is the use of the background theory for the development of a measurement tactic that will try to discover the ISA adoption level in the IT company, and the reasons why the employees of the company choose to adopt a certain behavior. After that the second objective is to create a methodology that adjusts the measurement findings to the ISMS of the company. The outcomes of the study will support the refinement of POST™ both as theory and as measurement tactic.

Delimitation of the thesis is that it is based only on the study of one IT company and the researcher makes the analysis of the data based on the background theory, so there’s a danger for a failure if the sample for the collection of data will be considered as poor and if the analysis of data will be considered as subjective. The IT company operates in the region of west Thrace in Greece and it has three branches in the biggest cities of the region. For the purposes of the research it was selected as a sample the head office of the company. So neither the outcomes of the measurement of the employees’ ISA adoption level nor the developed ISMS can be generalized for the whole company. Furthermore, as the time for the conduction of the research was limited it couldn’t be examined the effectiveness of the developed ISMS even to the company’s head office.

1.5 Thesis Structure

The first chapter constitutes an introduction to what ISA is and how critical is for the organizations, see Fig. 1.1. Also this chapter presents the aim of the study and the research questions in which this study has been built. The second chapter provides all the background theory for the conduction of the research in the IT company and analyzes its importance comparing to previous studies. The research method (philosophical Worldview, collection of data, analysis, etc) is presented in the third
chapter together with an argumentation about the validity of the research, the risks that are into consideration, the ethical context for the conduction of the interviews and the store or use of the collected data, and the translation process. In the forth chapter are presented the results of the analysis of data after the study in the IT company. Also this chapter contains an argumentation about the need of the refinement of POST™ framework and there’s suggested a methodology for the link of the measurement findings of the ISA adoption level in an organization to the development of ISMSs. The next chapter is a discussion about the empirical findings and the basic factors that contribute to the measurement of ISA adoption level in an organization (when based on the behavior of the employees). The sixth chapter concludes by reminding the key points of the thesis and gives the turn to the references and the appendices.

Figure 1.1: Thesis structure.
Chapter 2: Literature Review

Chapter 2 begins with a review of the previous studies that have addressed the research problem and discusses about their deficiencies. The chapter continues with the analysis of the background theories of POST™ framework and PEST analysis, and then with an explanation about how the above theories have been used for the conduction of the research and the provision of the final results.

2.1 Previous Studies that have addressed the Problem

Many studies have been conducted about the importance of ISA and about its relevance to the adoption of an ISP and the creation of an ISMS in an organization. Siponen and Vance (2010) acknowledge that ISA will help the employees of an organization to be compliant with its ISP. Furthermore, they point out that it is a responsibility from the supervisors to ensure that their employees are aware about the organization’s security policies and they completely understand their importance. Puhakainen and Siponen (2010) relate ISA with information security compliance and give focus to the training of the employees on IS. The authors also present several frameworks [created by Desman (2002); Lafleur (1992); Mitnick (2002); NIST (1996); Peltier (2002); Perry (1985); Telders (1991); Thomson and von Solms (1998); Vroom and von Solms (2002)] that suggest certain strategies for the implementation of information security training programs (ISTPs).

Eminağaoğlu, Uçar, and Eren (2009), after the completion of their quantitative research for the effective implementation of an information security awareness program (ISAPM) in a Turkish company, conclude to the fact that ISA is a mean to minimize the information security risks and that the information security awareness programs help the employees to accept the company’s ISP. Parsons et al. (2014, p.167) used hybrid research methods in order to create a questionnaire (named human aspects of information security questionnaire, HAIS-Q) for the measurement of the ISA adoption level in the organizations, while using existing knowledge from previous researches about internet use, email use, social networking site use, password management (including locking workstations), incident reporting, information handling and mobile computing.

Maqousi, Balikhina and Mackay (2013, p.66, 69-70) point the importance of the adoption of an information security awareness culture in an organization and they argue that the next step for the development of an ISP and an information security strategy is to apply their suggested information security awareness program. Their suggested program is based on Analysis, Design, Implementation, and Maintenance and it is expanded to further steps (identify, design, develop, implement, maintain, measure, review) in order to create a map for the initiatives, when they try to implement an ISAPM and measure its effectiveness. Tsohou et al. (2012, p.330) make use of the Actor-Network-Theory (ANT) so as to examine the role of ISA as socially constructed. Warkentin et al. (2011, p.268, 277) stress the need to link the informal training to the formal training programs and state about the informal social learning which is depended on the behavior of the individuals and the way that they understand what is wrong or not. Anderson  and Agarwal  (2010) get an insight into the problem of information misuse from the PCs of home users, and make claims about the high influence of the behavior of the users by social norms and by psychological factors.
Users’ awareness is depended on their behavior and that supports the argument that the IS managers have to define ISMSs that are adjusted to the behavior of their employees, as individuals and as a part of a group. Bulgurcu et al. (2010, p.541-542) relate the role of compliance, normative beliefs, and self efficacy to the formulation of the attitudes of the employees and the implementation of ISA in an organization. In addition, they state that the attitude of the individuals is the factor that forms the effectiveness of ISA and that the ISA defines the effectiveness of the implemented ISP. D’Arcy et al. (2009, p.91-92) acknowledge the importance of ISA for an organization and they built their statements on general deterrence theory (GDT), and they suggest the security, education, training, and awareness (SETA) programs. The authors argue that the severity of sanctions (and not the certainty of sanctions) may influence the information misuse (e.g. when the information misuse is related with the improper use of the PC), but the moral intentions of the employees are those that define the final decision to respect or not the organization’s ISP. Johnston and Warkentin (2010, 560-562) state that self-efficacy, response efficacy, threat severity, and social influence are the elements that define the employees’ behavior and their willing to comply with the organization’s ISP. They also argue about the effectiveness of fear appeals for the advance of an ISP, but they point out that the fear appeals are highly influenced by the human behavior.

Many researchers tried to indentify the relation of the psychology of the employees with their performance at work by the examination of the dependence of every psychological construct (as it has been determined and constructed by the psychologists) on their attitude at a working environment or on their attitude out of the working environment. The main focus of the above researches wasn’t to identify and define a psychological attitude and product theory about the human behavior, but to take it as standard attitude of a person and try to discover the expansion of this attitude when the end users adopt certain roles in life (e.g. information security manager). Kajzer et al. (2014, p.65-66) state that all the previous researches about ISA had as main themes the deterrence (formal sanctions to those that don’t respect the information security policies), morality (the ethical norms that characterize the personality of the individuals), regret (the emotions of the individuals define their final actions), feedback (positive or negative), and incentives (the provision of rewards to individuals). So the authors try to connect the above main themes of the previous studies (and their outcomes) with the key principles that formulate the personality of an individual (Big Five personality traits, Machiavellianism, Social desirability) in order to support their basic hypothesis that the personality of the employees affects their compliance with the organization’s ISP and defines the success of the organization’s information security strategy.

Myyry et al. (2009) try to identify the influence of morality (moral reasoning) and the influence of values to the compliance of the employees with an organization’s security policies and conclude that preconventional moral reasoning, as opposed to conventional moral reasoning (2009, p.127-128), is positively influencing the acceptence and respect of any security policy (e.g. the fear of punishment make the employees to be compliant with the ISP). Albrechtsen and Hovden (2010) argue that the personal contact of the IS managers with the employees of an organization and the communication of the ISP within small groups (i.e. to give the employees the ability to speak and reflect) will positively affect the advance of ISA as it positively affects the behavior of the employees. Kruger and Kearney (2006, p.291-292) construct a
prototype for the measurement of ISA in the organizations and stress that the main three factors that have to be measured, and can further analyzed in subcategories so as to define the adoption level of ISA are: knowledge, attitude and behavior.

Siponen (2000) argues that the IS managers of the organization have to ensure that their employees have fully conceived the meanings of the security messages and they have accepted it. In addition, Siponen (2000, p.32) argues that two psychological constructs influence the compliance of the users with ISP: motivation and attitude. Schultz (2005) stresses the need for the researchers to focus on the human factor, as people are those that affect the uses of the technology. Schneier (2000, 2012) tries to connect all the previous identified and well-structured knowledge of the field of psychology with IS, and builds his argumentation by relating attitudes and behaviors of the individuals with cases of information misuse. According to Layton (2005, p.6) the effectiveness of any information security strategy depends on the intent of the end users to adopt ISA. The implementation of ISA in an organization is based on the six psychological constructs that constitute the behavior of the end users: motivation, attitude, beliefs, personality, morals and ethics. These constructs cannot be directly measured as there are many factors that influence them, but there is an opportunity for the researchers to investigate them and to define measurement criteria for every psychological construct in an indirect way (i.e. when the researchers know and understand the theoretical background of every construct and try to examine the affection of every construct to the final decision of the end users to adopt ISA or not).

2.2 Deficiencies in the Previous Studies

Bulgurcu et al. (2010); Warkentin et al. (2011); Kajtazi, (2013) state that there are two approaches for the development of the organizational IS strategies: 1) the socio-technical or technical approach and 2) the socio-organizational approach. The former invests on the use of technology based solutions for the secure of the organization of possible threats. The latter depends on the behaviors of the individuals because it recognizes that the end users are those that define the protection level of the organization from a compromise of classified information, from a virus infection or from hackers’ attack. This thesis supports both the socio-organizational approach and the socio-technical approach and stresses that the behavior of the end users and their willing to accept the organizational ISP are the factors that define the ISA adoption level in an organization, but the organizations have to invest also in technology based solutions after they have ensured the awareness of their employees to IS issues and policies (Bulgurcu et al, 2010). All the previous studies that support only one of the approaches don’t take into consideration on the one hand the behavior of the individuals and their psychology which can lead them to the non respect of the organizational ISP despite the number of the IS technological artifacts that are in use (i.e. with the socio-technical or technical approach), and on the other hand the second approach studies the behavior of the end users and understands that the end users have to internalize the meaning of ISP but with the pass of time the technology based solutions are necessary because even the most cooperative employees may be unable to limit high tech attacks and threats with old fashion technology (i.e. with the socio-organizational approach).

Siponen (2000); Layton (2005); Webb et al. (2014) argue that the theoretical models of security awareness are the descriptive model and the prescriptive model.
According to Siponen (2000) and Layton (2005) the difference between the two approaches is that the prescriptive approach focus on the internalization of the meaning of IS and ISA by the end users and after that it focus on the adoption of ISA, while the descriptive approach focus on the development of ISP that will ensure the safety of the organization and will be supported by the organizational ISMS (e.g. sanctions for the non compliance with ISP). For Webb et al. (2014) the descriptive approach is built much in detail and it is similar with a complicated map that contains detailed information about policies, actions and procedures, but the authors find that the descriptive approach is more general and that it can be easily used together with other theories (i.e. the descriptive approach studies a phenomenon in general). The prescriptive model of security awareness is used for the needs of this study and it is stressed that the ISA adoption level of the individuals is highly affected by their behavior. The six psychological constructs of POST™ framework are those factors that formulate the behavior of the individuals relating their willingness to adopt ISA or not and every psychological construct can be influenced by intrinsic and extrinsic factors, so it is useless if the organizations just develop ISP and wait from their employees to be compliant with that policies, without to ensure that the formulated ISP are constructed according to the desires of the end users (Layton, 2005).

As it has been stated in paragraph 2.1, some previous studies measure the level of ISA while using some of the psychological constructs of POST™ framework and some other argue about the importance of some of the psychological constructs to the behavior of the end users, and how can these constructs affect their ISA adoption level and their compliance with the organizational ISP (Parsons et al, 2014; Maqousi, Balikhina and Mackay, 2013; Kajzer et al, 2014; Kruger and Kearney, 2006). Furthermore the psychology of the end users has been studied for the creation of ISTPs that will inspire the individuals and make them to be aware to the organizational ISP (Puhakainen and Siponen, 2010; Eminağaoğlu, Uçar, and Eren, 2009; Maqousi, Balikhina and Mackay, 2013; Bulgurcu et al, 2010), and some researchers (D’Arcy et al, 2009; Johnston and Warkentin, 2010; Kajzer et al, 2014; Myyry et al, 2009; Albrechtsen and Hovden, 2010) used the psychological constructs in order to discover their influence to certain ISMSs (e.g. strategies built on deterrence, fear appeals, etc…). Although the great advance to the IS field and the illustration of unexplored areas, the previous studies haven’t examined the six psychological constructs of the POST™ framework together in order to measure the employees’ ISA adoption level in an organization and after that to develop ISTPs and ISMSs. In addition despite the fact that all of the psychological constructs of the POST™ framework have been researched and it is generally accepted that they influence the behavior of the individuals and their compliance with the organizational ISP, there isn’t a study that tries to combine all the previous knowledge about the psychological constructs so as to examine the affection of the constructs to the behaviors of the individuals relating their willingness to adopt or not ISA. For the needs of the study in the IT company it is used the background knowledge of every psychological construct, so as to measure the level of the employees’ ISA adoption level and identify the reasons for adopting ISA or not. Also a PEST analysis of the measurement results is used as a filter in order to examine the affection of the external factors to the behavior of the individuals and the affection of the external factors to company’s businesses. The PEST analysis filter helps to understand if the external factors are the main factors that define the ISA level in the company and it also helps to develop an ISMS that will try to implement ISA in the company. In addition it is more easy for the IS managers to understand if the ISA
adoption level in their organization is high when they know that the negative external factors that affect the behavior of the end users don’t longer exist (e.g. when a country is under financial crisis and after some period of time it has a healthy economy). Another filter that is used for the measurement results (before PEST analysis) is the division among the end users that adopt ISA and the end users that don’t adopt ISA, so as to develop an ISMS that will satisfy both the two categories of the end users.

Despite the fact that the previous studies gave the IS managers the opportunity to reconsider the importance of ISA for the creation of ISP and ISMSs in their organization, they doesn’t provide them the opportunity to have access to knowledge that will help them to understand the psychology of the employees and to construct their ISMS in a manner that will be in high dependence with the employees’ behaviors. Also in the previous studies the researchers after reading the existing literature about the affection of the behavior of the employees to their working performance, they choose to use well constructed psychological theories while using subjective criteria of what suits better or not for the case, but Layton (2005) develops his framework and formulates six psychological constructs that contain all the respective literature about every construct and the researchers have the ability to combine two or more theories together so as to develop their measurement tactics. So it is used not only the theories that have been stressed from the other researchers as the most representative, but also there are used other additional theories about every psychological construct (theories that are referred to Layton’s framework). The key factor is to develop a measurement tactic that will examine in depth the correlation of every psychological construct (and all of the psychological constructs together) to the adoption of ISA by the end users.

The psychological constructs of the POST™ framework (Layton, 2005) are affected by internal and external factors. The internal factors that influence the adoption of ISA concern the internal world of the individuals and they can be “measured” by the development of measurement tactics that will be based on the framework. Although it is possible to measure the influence of the external factors to the behavior of the individuals, a PEST analysis will help the IS managers of the organizations to understand the relation between the external environment and the adoption of ISA. Through the PEST analysis the IS managers can examine the affection of the external environment to the employees’ behaviors and correlate their measurement findings with the additional findings. There is a possibility that the behavior of the individuals will not be the same through the pass of time (Johnston and Warkentin, 2010);(D’Arcy et al, 2009);(Siponen, 2000), so the IS managers of the organizations should arrange short measures to identify the ISA adoption level of their employees in order to adjust their ISMS to the new measurement findings (Layton, 2005). The PEST analysis helps also the IS managers to evaluate the external environmental factors and examine their influence to the adoption of ISA. Although the psychology of the individuals is affected by external factors, these factors may be different for every case.

An assumption is that the external environmental factors can perform a big amount of direct influence to the behavior of the individuals in several cases (such as a war, a financial crisis of an organization or a Country, a financial depth of an organization or a Country, etc) and after these factors stop to exist then the individuals may adopt their old behavior or create a new. The above assumption can be supported by the
motivational theory of Layton (2005) and the “pyramid” of Maslow, if it is considered that in the first step of the pyramid is the basic needs of the humans and that in some “extreme” environmental factors these basic needs cannot be covered by all of the people. Another assumption that leads to the need of use of the PEST analysis together with the POST™ framework for the identification of the ISA adoption level in an organization is that the political, economic, social and technology factors may influence the behavior of the end users in an indirect way. As it has been stated above the extrinsic factors contribute to the formulation of the psychological constructs of the behavior, so these extrinsic factors may be affected by the factors that are examined through PEST analysis or it may be affected by other factors that are influenced from the constructs of PEST analysis. A support for the above assumption can be Layton’s (2005) about ethics, for example if a communistic political party formulates a government in a Country then it will try to design communist ethics and these ethics will affect the end users (i.e. the political factor affects the psychological construct of ethics). But even the influence of the external environment to the behavior of the end users is indirect at first, it becomes direct with the pass of time and it has to be examined as a direct affection (i.e. the difference between the indirect and the direct way is the time that the behavior of the end users will be affected).

The purpose of the use of the PEST analysis is not the investigation of the affection of the constructs of PEST Analysis to the behavior of the individuals by a psychological perspective, but it is used to support the statement that the IS managers of the organizations have to conduct a PEST analysis together with POST™ framework when they try to measure the ISA adoption level in their organization. Also the PEST analysis is used together with the POST™ framework because it is estimated that it will give IS managers the ability 1) to evaluate the measurement results of POST™ framework and to understand the “why” in a better way 2) to adjust the measurement findings in their ISMS, and 3) to examine the “reliability” of their measurement and to arrange new measurements accordingly.

2.3 POST™ Framework

Layton (2005, p.3) introduces the psychology of security and technology (POST™) framework in order to help the IS managers of the organizations to identify methods for the development of ISMSs that will be adjusted in the psychology of the employees. The POST™ framework develops ISA in the organization by supporting the opinion that the key factor for its effectiveness is located in the psychology of the employees and their willing to cooperate. Furthermore, the framework is based on six psychological constructs: motivation, attitude, beliefs, personality, morals and ethics. These constructs can be used as a basis by the IS managers in order to develop measurement tactics that identify the adoption level of ISA in their organization and the desire of the employees to accept any ISP. Also the identification of the motives of the employees (in order to cooperate) will support IS managers to the properly adjustment of their ISMS and to attain their final goals about the compliance of the employees with the organizational ISP. The implementation of the POST™ framework in the organization has to be culturally and contextually desirable.

The framework doesn’t provide a standard theory or measurement tactics that are the same for all the organizations. Contrarily Layton (2005) stresses that the
framework can be used as a basis for several researches to build on and provide additional theory. The goal of the framework is to identify the level that the end users have internalized the meaning of the information security programs and intends to illustrate the reasons for not accepting the organizational ISP. For achieving the above purposes the POST™ framework tries to explain not “how” the end users comply or not with the company’s ISP but “why” they perform such behavior. Discovering the “why” makes it possible for the IS managers to adjust the ISTPs (or ISAPMs) of the company to the desires of the end users and to control their effectiveness with quick methods of measurement. Also if the IS managers of a company can understand the “why” (i.e. ISA adoption level of their employees) then they can develop an ISMS that will be incorporated to the overall strategy of the company and will not negatively affect its goals. After the measure of the ISA adoption level in the organization, it is suggested a PEST analysis in order to ensure that the developed ISMS won’t affect the culture of the company and the ways that it operates in the market.

Every psychological construct of the framework can interact and influence the others, see Fig. 2.1. This means that no one of the constructs of POST™ can be handled as an independent part and examined separately from the other constructs. Layton (2005) states that the psychology of the end users is something that can be influenced from several factors and despite the fact that someone fulfills the “requirements” of some psychological constructs so as to adopt ISA, on the other hand other personal or environmental factors can pressure the end users for not respecting the ISP of the company and not complete the “requirements” of other psychological factors. Every construct of the framework constitutes a category for research by the scope of the IS managers in order to understand the reasons that the end users tend to be aware or not with the organizational ISP. But after the identification of the “why” for every construct, the IS managers of an organization have to combine all the results for every construct, so as to create the whole picture of the ISA adoption level.

There is an interaction point that links all of the psychological constructs and forms their relationships. This interaction point is the point that every psychological construct is almost constructed so as to become a part of the framework, and this is the point that the other psychological constructs take action and start to influence the formulation of the others. It is important to be noticed that:

A. Every psychological construct is directly related with the framework:

The theories behind every psychological construct try to formulate the main theory of the framework and help to develop measurement tactics that identify the factors that affect them. The supporting theories can be used to understand the factors that contribute to the formulation of every psychological construct and understand the reasons for adopting or not an ISA in relation with this construct.
B. Every psychological construct is directly affected by the formulated framework:

The formulated framework helps to better understand the constructs because they are affected not only from the factors that are described in their supporting background theory, but also they are affected by other environmental, political, etc… factors and the gained knowledge about the other constructs.

C. Every psychological construct interacts with the others to formulate the framework:

The formulation of every psychological construct is directly affected by the other constructs. None of the constructs can be isolated from the others and examined separately. It is tried to be developed a complete picture of the problem, so the framework helps to discover the means to explain the human behavior relating the acceptance of the end users with the company’s ISP and it helps to measure their ISA adoption level.

D. Every psychological construct is affected by the other constructs of the formulated framework:

As it has been stated above the formulated framework affects every construct and helps to examine it in a better way. In the same way the examined constructs of the formulated framework help to better understand the other constructs and take into
consideration an extended context of parameters, so as it can be developed measurement tactics that try to combine the gained knowledge with the old one.

Fig. 2.2 is similar to Fig. 2.1, but it presents the relation of the psychological constructs with the human behavior. Also it provides an insight to the POST™ framework background theory and it helps to understand that every psychological construct affects alone and together with the other constructs the human behavior, and that every construct is influenced by the other constructs. The definition of the above statement creates the need to examine the way that all the psychological constructs affect the desire of the end users to adopt a behavior that will be compliant with the organizational ISP, so Layton (2005) developed the POST™ framework in order to help the IS managers of the organizations to measure the ISA adoption level of the employees in their organizations and after that to define ISMSs.

Layton (2005) bases his background theory of the POST™ framework to the existing knowledge and the findings about the organizational citizenship behavior (OCB). More specifically the author understands that OCB helps to better understand the behavior of the employees in an organizational context and argues that the employees adopt their behavior depending on their motives. The motives of the end users are very critical for the adoption of ISA and are affected by the aspects of human behavior. Seven categories of OCB are the most common, see Fig. 2.3 (Podsakoff et al., 2000); (Layton, 2005, p.37):

- **Helping behavior**: OCB provides the theoretical background to understand the behavior that is advanced not only from the employees that are obligated to help the
other employees as this is one of their working duties, but also it is cultivated from the employees that are not obligated to help the other employees. The second type of the employees that help the others because they are motivated by their feelings, their beliefs, their ethics or by their good working environment, etc… adopt the common called extra-role behavior. The extra role behavior is affected by the psychology of the end users and this is the reason that Layton (2005) correlates it with the POST framework and tries to use it as a background theory, although the extra-role behavior needs to be more investigated.

- **Sportsmanship:** although this category is underestimated and not fully explored, it helps to understand the behavior of those that accept to do anything that they’re asked to do without complaining. This category is related with the employees’ desires for a good carrier and a stable working environment. The problem is that the organizations today don’t offer carrier commitment and they operate in an unstable market environment (Layton, 2005, p.38).

- **Organizational loyalty:** this category is related with the success of the organization’s operation activities in the marketplace (now and in the future) and its economical stability. The organizational loyalty is also related with POST™ framework because it can provide a background theory about the relation of the employees with their organization, a relation that is affected by the perceptions and the expectations of the employees (Layton, 2005, p.39).

- **Organizational compliance:** this category of OCB is related with the desires of the employees to be compliant with the organizational norms and policies. It is highly related with POST framework because it helps to understand the reasons for compliance with the organizational ISP (Layton, 2005, p.39).

- **Individual initiative:** this construct of OCB helps to understand an extra-role behavior that is advanced by the employees of the organizations when they offer in a voluntary basis their services to others or when they try to be innovative. Also it helps to understand the limits that are placed by this kind of the employees when their motives are in contrast with the organizational ISP (Podsakoff et al., 2000); (Layton, 2005, p.39).

- **Civic virtue:** it is the willing of the employees to be a part of the organization and participate to the organizational meeting, to express their opinion about any theme that they feel it is critical for the organization, to cooperate in researches that try to improve the organizational procedures, etc…This construct helps to understand the adoption level of ISA that is adopted in any case even when the employees present a sympathetic behavior or a disdain behavior (Layton, 2005, p.40).

- **Self development:** it is the willing of the employees of the organization to improve themselves in the fields that they feel that are important (e.g. to be better at work, to obtain more knowledge about something, etc…). Layton (2005, p.40) argues about the connection of this construct of OCB with the extra-role behaviors and stresses the need for further research.

Layton (2005) stress the need to examine the extra role behavior as it can help the IS managers of the organizations to develop ISMSs that enforce the relations between
the members of a group and the relations between the working groups. Also the examination of extra-role behaviors (together with in-role behaviors) provides the opportunity to evaluate the behavior of the end users on a regular basis and through the pass of time. In addition the extra-role behavior helps to understand the level that the employees are satisfied with their working environments and the level of their compliance with the organizational norms and policies. This part is very critical for the IS managers as the compliance of the end users with the organizational policies is highly related with their ISA adoption level.

The POST™ framework has been introduced by Layton (2005) and the author argued that it has been developed in order to become a tool from the IS managers so as to access the adoption level of ISA in their organizations. According to the author the framework cannot be used only as theory because it has to be examined by the researchers first with the pass of the years and reformulated when needed, and then after the use of the framework for the conduction of many researches and after its improvement as a measurement tactic, it can be used both as theory and as a measurement tool. A further analysis of the framework’s psychological constructs is provided in the paragraphs below.

Figure 2.3: The most common categories of OCB (Podsakoff et al., 2000);( Layton, 2005).

2.3.1 Motivation

This psychological construct concerns the motives of the end users that make them to adopt a certain behavior. At first it was considered that the motives of the humans
were their physiological needs (i.e. food, water, home, sex, etc...) but with the pass of the time it was discovered that the humans can behave in some way depending on their intrinsic motivations. The term intrinsic motivation is relative with IS because it is important in the information security field that the end users internalize the meanings of the information security messages (Siponen, 2000). The theories that are considered as the most representative for this construct are: Need Theory, Two-Factor Theory, The Operant Model, Goal-setting Theory, Expectancy Theory and Equity Theory (Layton, 2005, p.53-54), see Fig. 2.4.

**Figure 2.4: Theories of motivation.**

- **Need Theory**: this theory concerns the well-known to the managerial field of knowledge as Maslow’s Pyramid (Maslow, 1943);(Layton, 2005, p.54-57). This pyramid contains five levels and every level represents the needs of the humans in order to be completed as personalities. The first level of the pyramid is the **physiological needs** of the humans (e.g. water, food, home, etc) and stresses that these needs are the first priority for all the people. The second level of the pyramid are the **safety needs** (e.g. safety at home, in the working environment, etc). This step is in great relation with the IS field because it is expected that if an employee doesn’t feel safe in his organization and he is afraid all the time for losing her/his job, then it is very difficult for her/him to respect the organizational ISP. The third level is the
social needs (i.e. the desires of the humans to be in love, to have a family, to have friends, to be liked by the others, etc) and the level after is the ego needs (i.e. the need to be successful and strong, the need to have freedom, the need to be autonomous, etc). The forth level is in high relation with the IS field as it has been discovered that there is a higher adoption of ISA if the employees feel autonomous to act than if they are afraid of sanctions (Deci, 1996);(Layton, 2005). The last level of the pyramid is the self-actualization need and concerns the need of the humans to become what they dream to be and to do the best to attain it (Layton, 2005).

- **Two-Factor Theory**: Herzberg (1966); (Layton, 2005, p.58-60) introduced the Two-Factor theory which is actually a theory that tries to discover the motives of the humans and understand their behavior. This theory also posits the needs in the surrounding environment of the humans and not into their internal world. The latter is in contrast with the IS field and the belief that the internalization is the main factor that determines the behavior of the end users, but the theory is examined because it provides critical knowledge about the affection of the surrounding environment to the human behavior. The name Two-Factor has come from the assumption that the bad working behavior is related with the dissatisfaction and the positive working behavior is related with the satisfaction of the employees. It has been discovered that the intrinsic factors lead to the satisfaction at work (e.g. when the employees feel that there is an advance and a progress relating to themselves and the organization) and that the extrinsic factors are associated with dissatisfaction at work (e.g. organizational policies that are not friendly to the employees). The extrinsic factors are in relation with the IS field because it can help to discover the dissatisfaction of the end users that don’t agree with the organizational ISP.

- **The Operant Model**: this model is critical for the POST™ framework because it is related with the high level of the ISA adoption by the end users that are working in an environment that helps them to respect the organizational policies. The operant model is based on the reinforcement, meaning that the IS managers can “reinforce” the positive behavior of their employees with awards (i.e. bonus to the salaries, positive attitude to those that respect the ISP, etc) and a good working environment. Other parameters are the positive or negative feedback from the IS managers to the employees of the organization depending on their behavior and the punishment of the employees that perform a negative behavior (i.e. don’t respect the organizational ISP). On the one hand according to the operant model the positive reinforcement of the employees is the “valued rewards” (i.e. everyone takes what she/he deserves to take depending on the actions that she/he has done) and the positive feedback. On the other hand the negative reinforcement is related with the sanctions and the negative feedback (Layton, 2005, p.60-64).

- **Goal-setting Theory**: according to this theory there is necessity from the managers of the organizations to set goals that will be compliant to the employees’ desires and they will be considered as attainable. This theory is related with ISA because the above necessity is the same for the goals that are set by the IS managers and are related with their ISMSs. Layton (2005, p.65-68) states that the IS managers have to define the IS program’s goals and the organizational goals and after that they have to monitor and define measurement tactics so as to discover the compliance of their employees with the goals that have been set. Also the author stresses that the ISP of every organization are built on specific goals, so the employees have to be complaint
with these goals and they have to internalize their meaning in order to adopt a high level of ISA.

- **Expectancy Theory**: the expectancy theory is used in the POST™ framework so as to investigate the extrinsic factors that are related with the perceptions of the end users which determine their ISA adoption level. According to this theory the employees adopt a certain behavior according to their perceptions (e.g. awards, good working environment, etc) and they tend to be compliant with the organizational goals, norms and policies when they feel that the organization has covered their expectations. There is a great relation of this part of theory with the psychological constructs of ethics and beliefs, as the perceptions of the individuals vary in every case. The IS managers have to develop ISTPs that will be based on moral reasoning so as to cultivate ethical cultures in their organizations and this is a point that has to be measured according to the POST™ framework (Layton, 2005, p.68-71).

- **Equity Theory**: this theory is used by the POST™ framework so as to examine the social justice between the employees of an organization. The social justice is an extrinsic factor that affects the behavior of the end users. The unfair treatments of the employees (e.g. different rewards for the same action) are connected with the employees’ dissatisfaction and they influence their ISA adoption level. But when the employees feel that they are treated by their IS managers in the same way like their fellows, they tend to adopt a more complaint behavior to the organizational ISP (Layton, 2005, p.71-72).

2.3.2 Attitude

The attitude of the individuals is all those feelings, beliefs, intentions and statements about something which affect their final behavior. The POST™ framework studies the attitude so as to enable the IS managers to construct psychology-based measure tactics that will examine the ISA adoption level in their organizations. After the examination of the intrinsic and extrinsic factors of attitude that lead to the adoption of ISA, it is possible for the IS managers to develop suitable ISMSs (e.g. the employees will be compliant with the ISP of the organization). Organ and Bateman (1986); Layton (2005, p.79) argue about three components of attitude: affective, cognitive and behavioral. The affective component investigates the feelings that are caused to the end users when they hear or read some words. Layton (2005) states that the IS managers have to develop the ISP of the organization in a manner that they will contain neutral words (i.e. words that will not make the employees to feel uncomfortable or have negative feelings) and this is something that has to be searched through the POST™ framework. The cognitive component of attitude is about the beliefs of someone for something. It has been identified that the adoption of a certain style of attitude in a situation is related with what someone believes about the actors and the environment of that situation, so it is important in the IS field to discover the opinions of the end users about the ISP of the organization and the IS in general. The behavioral component of attitude connects the attitude with the behavior and points out that the attitude of someone is depended on several factors (such as the environment, ethics, etc...), so the end users will adopt a certain behavior about something cause of their attitude about the same thing (Layton, 2005, p.79-81).
2.3.3 Beliefs

The psychological construct of beliefs presents the feelings of someone about something and the level of its internal acceptance. The beliefs are the thoughts of the individuals about the word around them (e.g. actions, statements, theories, etc…) and they are expressed through their behavior. The POST™ framework suggests that the IS managers of the organizations need to identify the beliefs of their employees because on the one hand they will understand the way that their employees behave and on the other hand they will afford to develop their ISMS according to the “desires” of their employees. The beliefs are related with the internalization of the meaning of IS and the compliance with ISP. If the employees have negative beliefs about the organizational rules and norms, then it is reasonable if they don’t adopt ISA. Furthermore, the measurement of this psychological construct through the framework context is very critical as according to epistemological theories the beliefs are related with the individuals’ motives and attitude (Layton, 2005, p.94-97).

2.3.4 Personality

There are many definitions about personality and many researchers tried to understand its components and the factors that affect it. Layton (2005, p.82) places personality as the answer to who we are and why we are the same we are. The personality of a person is influenced by several factors such as the environment, the education, the ethics, the beliefs, the social status, etc…In recent time has given great interest to individualism, a term similar to personality that concerns the study of a person’s individual personality and not the study of a person’s personality as a part of a group (no matter if the type of the group is the race, the party, etc). The personality is something unique and everyone has a different personality from the others, but it is a psychological construct that is consisted of several components that can be altered through the pass of time. In other words the personality is built with the use of many layers and every layer has its own characteristics. Some of these characteristics usually stay in their initial form through the pass of time and under several circumstances, and don’t alter the type and the form of the layers that they are part of (e.g. sexual preferences). But some characteristics alter the layers that are part of when they are influenced by extrinsic or intrinsic factors and then they change also the behavior of the individuals (e.g. preference to the fashion style that is going to be adopted).

Personality is a psychological construct which helps to understand a person as a whole (and not separately each of an individual’s components) and explains the way that this person behaves. It helps also to discover the emotions, feelings and thoughts of a person and this is very critical for the IS field as these components usually don’t alter through the pass of time. The two main categories for personality is the core personality, which tends to be stable through the past of time and the dynamic personality, which can be altered in dependence with the level that it is influenced by intrinsic and extrinsic factors (Layton, 2005, p.87).

- **Motive-based Approach:** As it has been stated in paragraph 2.3.1 the behavior of the individuals is driven by their motives. This approach investigates the relation between the motives and the behavior, and tries to identify how the motives affect the final decisions of the individuals. There are motives that have short time ending, but
there are also motives that exist for a long period of time. As this approach is located by the psychologists in the research area of personality, it has been decided to be incorporated in the framework of Layton (2005) cause of its great relation with the psychological approach of motives. POST™ framework is built on three layers: the first is morals and ethics, the second is personality, attitude and beliefs, and the third is motivation. The motivation is one step before the final definition of the behavior, as the motives highly influence the behavior of the individuals (Layton, 2005, p.88-89).

- **A Trait-based Approach:** this approach is different from the other as it gives focus to the comparison of people by the use of aspects and degrees. Gordon Allport, a trait theorist (see in Layton 2005, p.90), states that every person’s personality has its central traits which are basic components of personality that last with the pass of time and the occasional cardinal trait which is the “strongest” trait among all the other central traits. The traits are influenced by external factors (e.g. the environment), they born in the early ages of the people and mature when they grow. The most common traits that are considered as the main impediments of personality (known as the “Big Five” traits) are: 1) openness to experience (be open to discover new things, 2) conscientiousness (the continuum of the characteristics of people that make them to be either careful, organized, responsible, etc…or make them to be careless, not helpful, less responsible, etc…), 3) extroversion (the willing of people to do things and cooperate with others)/introversion (the willing of people to do things on their own or in short groups), 4) agreeableness (to help, trust and understand the other people and try to cooperate with them by making the things easy), 5) neuroticism (the level of the emotional stability), the higher level of neuroticism presents a higher level of emotional instability (Layton, 2005, p.90-91).

The personality’s types and approaches are illustrated in Fig. 2.5. Despite the fact that at their beginning the two approaches (motive-based approach and trait-based approach) were examined separately, nowadays the researchers have discovered that the two approaches are very relative, and try to combine them so as to develop measurement tactics (e.g. questionnaires) that will examine the affection of personality to the behavior of individuals. Also it is important for the POST™ framework that the traits last for a long period of time and that gives the ability to define tactics, so as to measure those traits that affect the personality in an organizational setting (Layton, 2005).
2.3.5 Morals

The morals of the individuals define the final answer to what is wrong or not. This construct is used by the POST™ framework because it affects the behavior of the individuals. It is presented an absence of moral reasoning in the IS field and the individuals many times don’t understand the ethical dimension of the ISP. Layton (2005, p.119-122) states about two moral theories: *the Kohlberg’s moral development* and *the Gilligan’s moral growth*.

According to Layton (2005, p.119-120) the moral theory of Kohlberg has three dimensions: 1) preconventional, up to age 9 (a. *punishment and obedience*, it is observed for example when the children obey the rules so as to avoid the negative
consequences and b. egoism, for example when the parents cover their children’s egoism because they believe it is moral), 2) conventional, age 9 (a. when the children understand their obligations to their parents, teachers, etc. and try to be good/nice and b. uphold society, when the children understand their obligations to the society), 3) postconventional (a. social contract, i.e. the individuals’ opinions about what is moral or not start to differentiate to each other, b. conscience and universal principles, i.e. when the individuals judge the morality of others according to their own values of morality).

In addition, according to Layton (2005, p.121-122) the Gilligan’s moral growth is similar to Kohlberg’s moral development but it examines the moral issues by implementing an additional care perspective. Gilligan’s moral growth has the dimensions below: 1) preconventional (self-centered, the individuals seek to cover and satisfy their needs) 2) conventional (self-sacrificing, the individuals seek to cover and satisfy the needs of others) 3) postconventional (mature ethic of caring, the individuals seek to deserve a balance in covering and satisfying their needs and the needs of others).

Figure 2.6: Representative theories for Morals.
2.3.6 Ethics

Ethics represent the moral judgment of the individuals’ behaviors, so as to define them as “good” or “bad”. The ethics come also from the individuals’ beliefs about how the world should be and how the humans should behave in that world. This psychological construct is used by the POST™ framework cause of its great influence to the behavior of the individuals, thus it is one of the measurement criteria that define the employees’ ISA adoption level in an organization. Respective ethical theories that have to be in mind when using the POST™ framework are presented below (Layton, 2005, p.99-118):

- **Psychological and ethical egoism**: this ethical theory is related with the desire of the individuals to do things only for themselves (self-interest) and try to cover their needs no matter if their actions will harm the others. The problem with this theory and the human that accept it, is that anyone who adopts a psychological and an ethical egoism will try to cover her/his own needs and that many times this decision will cause conflicts (Layton, 2005, p.99-100).

- **Deontological Theories**: Layton (2005, p.100-104) makes a review of the literature about ethics and concludes to the fact that deontological theory concerns the adoption of a behavior that is committed to obey the moral values, laws and norms which define which actions are right to be done and which actions are not. The individuals that adopt a deontological behavior act for the common good and try to service the others as themselves, while trying at the same time to make their actions a universal law. The IS managers of the organizations have to indentify which of the employees believe in deontological theory, and try to understand the context of their beliefs related to what is right or not in the IS field (e.g. is it right to monitor the employees so as to find who don’t respect the ISP of the organization?).

- **Utilitarianism**: this category of ethics proposes to the individuals to behave in a way so as to satisfy with their actions the biggest amount of the people. It is a continuous comparison of the ads and the consequences of every action and the final decisions are taken when it will be accessed that they will be acceptable by the majority of the human population, no matter if the decisions are immoral from a deontological point of view (e.g. if the non respect of the ISP is considered as normal behavior from the greatest number of people, then the employees who believe in utilitarianism will not be compliant with the ISP of the organization). The utilitarian seek to enjoy positive feelings (happiness) and avoid the negative feelings (suffer) and this is the context into they build their morality. When the utilitarianism is applied directly by the selection of a certain action (among others) in a situation, then it is called *Act-Utilitarianism*. But when the utilitarianism is applied so as to define the validity of the manner in which people behave (by a moral perspective), then it is called *Rule-Utilitarianism* (Layton, 2005, p.104-105).

- **Contractarian Theory**: this theory focus on the contradictions between the ethical point of views of the individuals, as a result of their different social statement and duties. Layton (2005, p.107-108) stresses the importance of this theory as the organizations have to protect themselves from an IS leakage by acknowledging that there is a danger to be infected from *different* people who can live in *different* places, have *different* social status between them and adopt a *different* code of ethics.
- **Ethics and the internet**: Layton (2005, p.108-111) presents the RFC (request for comment) 1087 which is about the properly use of internet. As a properly use of the internet can be considered the use of the internet for authorized actions, the respect of the privacy of the others, the avoidance of the access to data resources without permission, the respect of the cultural and ethnical differences of the other users, the avoidance of creation or transition of viruses, etc...The POST™ framework examines this ethical point of view as many organizations act through the Web or have access to it.

- **Ethics and Information Technology (IT)**: the ethical view of the use of IT concerns not only the properly development and implementation of the technology but also the right use of it. Despite the fact that the technology offers solutions for security in the IT field, the key factor that leads to IS holds upon the users of IT. The users have to adopt a moral and ethical behavior so as to avoid putting their organizations in danger. Layton (2005) argues about the high advance of the technology and the innovations in the IT field and stresses that the *wisely* use of the computers and the technology is what defines the success of the new technological artifacts. The ethics in the IT field are not rules, norms or policies as the employees of the organizations are free to choose their behavior, but the ethics in the IT field try to influence the end users so as to make the right decisions (e.g. they can learn about the human rights, the virtue ethics, the feministic ethics, etc...). The IS managers of the organizations have to study the field of ethics in IT (while using a phenomenological perspective) so as to understand the different opinions of the employees relating to what is right or wrong with the use of the technology and how can the technology be creative (Layton, 2005, p.111-117).

- **Ethics in the workplace**: the development of organizational ethics is something difficult for the IS managers, as they need to develop ethics that will be accepted by the end users (i.e. the employees will agree to which behavior is “good or wrong”). Great focus needs to be given to the internalization of the meaning of the organizational ethics by the end users, so as not to be considered as additional norms and rules (Layton, 2005, p.117-118).

### 2.4 PEST Analysis

The organizations are affected by external environmental factors, thus they have to examine and analyze these factors before the development of their strategies so as to avoid possible threats. The PEST analysis studies the political (together with the legal factors), economic, social (together with the ecology factors) and technology factors. These environmental factors are considered as the most important cause of their influence to the organizational procedures and their ability to change with the pass of time (Ward and Peppard, 2002). Gondal (2004) makes use of the PEST analysis in order to identify uncertainties and risks of the external environment that can be caused by political factors, economic factors, socio-cultural factors and technology factors. Chaffey and Wood (2005) state that PEST analysis is a *traditional* strategic approach that helps for the assessment of the external environment of business. The authors also argue that the PEST factors are similar to the SLEPT (social, legal, economic, political and technological factors) factors. For Clarke (2001, p.101) the PEST analysis is a mean for the examination and analysis of the *opportunities and the*
threats that are born in the political, economic, social and technical areas of organizational actions.

- **Political (together with the legal factors):** the policies of the government of every Country can influence the organizational operations and strategies. Also the operations and the strategies of an organization can be affected from the policies that are promoted from the international companies. The managers of the organizations need to be aware of the policies of the government and the legislation of the Countries that the organization acts, in order to identify the opportunities that are born for their organizations (e.g. low taxation, enforcement of the small enterprises with free advising from specialists, etc…) and the context of technology use (e.g. development of policies for personal data protection) for the organizations and for the customers. (Chaffey and Wood, 2005). According to Ward and Peppard (2002) the political stability and the geopolitical stability are also factors that influence the organizational operations because they construct the nexus of the relations between the Countries (i.e. global trade without barriers, flexible legislation, etc) and they create a base for further organizational advance. In addition the authors stress the need for the alignment of the organizational businesses or e-businesses with the legislation of the Countries in which the organizations act (so as to ensure the privacy of their costumers and the protection of their personal data, to avoid double taxation of their products, to avoid threats and possible frauds, etc…).

- **Economic:** Ward and Peppard (2002) argue that the existence of free market has brought an economical advance and it has changed the trade rules (e.g. it is possible for an organization from one Country to buy products from another Country in lower costs), but the depth of a financial system influences the economical statement of the Countries and the organizations that used to make profits from that financial system in the past (e.g. monetary crisis of Argentina in 2001 and Greece in 2009). Furthermore Ward and Peppard (2002, p.72) state that the strengths of different currencies, inflation rates, money market rates and tax legislation are factors that can formulate the markets, can develop new markets and can define the business operations. The Authors also state that the advance of the web and the high use of internet have resulted to the development of new markets which invest to e-businesses. Chaffey and Wood (2005) argue that the implementation of new technologies (e.g. communication) and the use of the web for e-businesses in a Country are affected by its financial strength.

- **Social (together with the ecology factors):** According to Ward and Peppard (2002) the social factors are related with the increasing number of the employees that get into retirement and the increasing average of human life time, as the governments and the organizations need to provide pensions and health insurance for longer period of time. Also the governments have to provide strategies that adjust the public sector (buildings and procedures, taxation, health-care provision) to the needs of the eldest, and the organization have to develop strategies that will take into consideration the preferences of the eldest. Another social factor that is stressed by the authors is the social inclusion/exclusion relating with the use of the technologies and the internet (i.e. the inability of the older people to use the internet or the technology). Chaffey and Wood (2005) connect the social factors with the relationship between the new technologies and the people, and stress the need that the organizations have to examine the level of the costumer approval before the development of new
technologies and the level of their usage after the development. Another social factor for the authors is the advance of the communication technologies and the differences among those who use new technological artifacts and those that choose to use traditional technologies. The organizations have to protect their communication channels in their internal and their external environment. Gondal (2004) relates the social factors with the cultural factors and examines them together in the same category of PEST analysis.

The ecological factors that are examined through the PEST analysis focus to the protection of the environment. There is a great concern recently about the green movements and the green policy all over the world. The advance of internet made it possible for the environmentalists to “commercialize” their statements and their actions more easily than they did in the past. Many political parties hold their existence to the protection of the environment and many people vote these political parties. New opportunities are born for the organizations to expand their operation fields to new businesses and this is something positive for the society as there are provided new job opportunities (Ward and Peppard, 2002).

Figure 2.7: PEST Analysis.

- **Technology**: the managers of the organizations need to search the new trends in technology and try to implement new technological artifacts that will be aligned to the organizational strategies. Many managers evaluate the costs and the profits of a new technological artifact before its adoption, others make use of the new technology without planning, and others adopt the new technology followed by their enthusiasm and don’t analyze the pros and cons in detail. The key factor is to wait before any new step and analyze in detail the purposes of use of the new technology and the possible risks of any use (Chaffey and Wood, 2005). The technology is in great advance and it
will continue to be in future. New technological trends will come into the surface and the organizations need to be aware of any innovation with the use of reliable information. The organizations can influence the market and the governments of the Countries in which they operate (e.g. for their legislation, their tax system, etc…) by the creation of groups, lobbies or associations (Ward and Peppard, 2002, p.76-77).

2.5 Use of the Literature

In this research it is presented the necessity of the development of measurement tactics that will help the IS security managers to arrange short measures in order to identify the ISA adoption level of the employees in their organization. The theory of POST™ framework (Layton, 2005) helps to that direction as it contains theoretical tools which provide IS managers the opportunity to understand the reasons (according to their behavior) that the employees respect or not the IS issues in general and the ISP of their organization. PEST analysis (Ward and Peppard, 2002);(Chaffey and Wood, 2005) can be used after the measurement of the ISA adoption level in an organization so as to help IS managers to identify the external factors that mostly affect the behavior of the employees and their willing to be compliant with the organizational ISP. Also PEST analysis helps IS managers to “deal” with the external factors and develop suitable ISMSs. The developed ISMSs will be based on the measurement findings and will try to internalize the meaning of ISA to the employees. But if this cannot be happen then the developed ISMSs will try to implement ISA in the organization while trying to use strategies that will be based on the behavior of the employees and will “enforce” them to respect the organizational ISP. The importance of using well defined psychological constructs, which can help to identify the reasons of adopting ISA and can support the IS managers of the organizations to arrange measurement tactics and develop ISMSs, has lead the researcher to the use of POST™ framework. Also the importance of the evaluation of the measurement findings and their correlation with political, economic, social and technology factors constitutes the reason of using PEST analysis.
Chapter 3: Methodology

Chapter 3 begins with a presentation of the philosophical worldview upon which the research has been built. It continues with a description about the setting and the strategy of the research, the methods for the collection and the analysis of data, and the validity and reliability of the research results. The chapter ends with some ethical considerations about the conduction of the study and then with an argumentation about the translation process.

3.1 Philosophical Worldview

Chua (1986); Klein and Myers (1999); Myers (1997); Myers and Klein (2011); Orlikowski and Baroudi (1991) state about the existence of three research epistemologies or “paradigms”: positivist, interpretive and critical. Myers (1997) and Klein and Myers (1999) stress that qualitative research is not a synonym to interpretive research, and Myers (1997) argues that qualitative research can be positivist, interpretive and critical also. Orlikowski and Baroudi (1991, p.5) argue that for interpretive research the humans create their own subjective and intersubjective meaning for the world they live in, so the researchers try to investigate the phenomena while examining them from the viewpoint of the people that are connected with these phenomena. Also the authors argue that neither the objectivity of the phenomena, nor the generalization of the research results to a bigger amount of population exist for interpretive research, and that its focus is to place the participants in the center of the interest and understand the deeper structure of the phenomena by the shared meaning that the participants give to these phenomena. In addition, Orlikowski and Baroudi (1991, p.13) state that the social context and the social interactions affect the understanding of the “reality” and determine the level of the “gaining knowledge”, thus the interpretive researchers need to examine the social interactions of the participants as members of a group or not in order to understand the “why” (i.e. meanings, beliefs and intentions) of their social actions and the “why” of their performing behavior in turn.

Klein and Myers (1999, p.67) stress that interpretive research is valuable to the field of information systems (management and development) as it helps to examine and understand the way that people think and act in social and organizational contexts. Also they state that it is better to be based on some criteria when conducting and evaluating interpretive research so as to avoid possible risks of undesirable judgments, thus they suggest seven principles (coming from the background theory and philosophy of 1. anthropological research and 2. phenomenology-hermeneutics). Walsham (1993); Klein and Myers (1999, p. 69) states that the interpretive research in the information systems field focus on the understanding of the context of the information system and the ways that the information system affects and is affected by the context. The interpretive research in the information systems field is based on the fact that the understanding of reality depends on social constructions (i.e. language, consciousness, shared meanings, documents, tools, etc...), and on the fact that the relations between humans and their external environment can change with the pass of time (Klein and Myers, 1999, p.69). Qualitative research is fundamentally interpretive, as the researcher will collect and analyze the data while using personal criteria which are affected by sociopolitical and historical factors that exist at the time of the conduction of the research (Creswell, 2009, p.208). The decision of the
researcher to conduct or not interpretive research is influenced by her/his philosophical assumptions and by her/his “internal meaning of the reality” (Myers, 1997, p.4-5).

The underlying philosophical worldview behind this interpretive study lies on the examination of the participants’ social context and the relations between the social structure and the “reality” of the employees. The examination of the relation between people, their social environment and the other external factors that influence their everyday life gives the ability to understand the “why” of human behavior. Also the internalization of the meaning of ISA by the employees is the base of the background theory (prescriptive approach) which helps for the collection and the analysis of data. The measurement tactic that is used for the investigation of the ISA adoption level in the IT company intends to uncover the internal thoughts, beliefs and feelings of the employees about ISA. As the researcher believes that the employees and their understanding of the necessity of ISA in the company are the keys to gain knowledge about the reasons that affect their final decision to adopt ISA or not, great focus is given to the identification of the internal (i.e. meaning the factors that are related with the psychological constructs of POST™ framework that constitute the behavior of the end user who decides to adopt ISA or not) and external factors (i.e. meaning the political, economical, social and technology factors) that influence their behavior and determine their ISA adoption level. Thus, believing that the internal factors and the external factors affect the behavior of the employees and the level that they internalize the meaning of the IS issues and policies of the company, it was decided that the nature of the study would be qualitative and more specifically interpretive (Myers, 1997).

Interpretive research is forced to hunt a moving target as the internal and the external factors that influence the behavior of the individuals can change from time to time (Walsham, 2006). The measurement tactic that is based on POST™ framework is taking into consideration the above statement and helps IS managers to arrange short measures from time to time, so as to identify the ISA adoption level in their organization. Furthermore the PEST analysis helps IS managers to better understand the external reasons for not compliance with IS issues and ISP, and develop new ISMS when these external factors stop to exist. The measurement tactic of POST™ framework is not depended on a certain context and the psychological constructs cannot be measured with the use of quantifiable criteria (i.e. like in the measurement tactics of the positivist paradigms), but they can only be measured in an indirect way by the examination of the end users’ knowledge about ISA and the “reality” of the individuals about ISA.

The qualitative type of research was preferred in contrast to quantitative methodology. Many reasons can influence the final decision of a researcher to conduct a certain type of research, but in this case the main reason for the selection of this type of research was that through qualitative research there’s the ability to interact with the stakeholders and to better understand their opinions about the researched phenomena. Myers (1997) states that the ability to talk with the stakeholders helps the researchers to better understand the humans and their surrounding social and cultural environment. So through the conduction of a qualitative type of research it could be investigated the ISA adoption level of the employees, if the employees acknowledge the importance of IS issues and ISP, if they are compliant with the company’s ISP,
and the most important it could be examined the reasons that influence their final behavior.

3.2 Research Setting

The IT company is a high technology company which acts in the region of West Thrace in Greece since 1998. It has three branches in the largest cities of West Thrace, but its head office selected as representative sample for the purposes of this investigation. All the information about the IT company have been imported from its official web site, but neither the name of the company, nor its web site can be referred as this is the desire of the IT company’s IS manager. The IT company’s purpose is to provide solutions depending on the needs of its customers, and among its main activities are: 1) the provision of integrated IT solutions for every business, organization and professional, 2) the services of "Information Officer" with studies and implement projects in advanced technology, 3) the marketing, production, installation, maintenance and technical support of computer systems and networks 4) the training and related activities on new technologies, 4) providing connectivity services (telecoms and internet) and web services, 5) the development and promotion of software products (ready packages, custom apps, apps - internet services), 6) research into new technologies and participation in European programs. Thus, it attains its goals by: 1) the development of integrated solutions and proposals to make it more easy and convenient technology, 2) daily involvement in the subject of its activity, 3) the communication of its “message” and its capabilities to companies, organizations, professionals and individuals in the region of West Thrace, 4) skills development and expertise of its partners to achieve the best possible use of technology, 5) the diffusion of information and knowledge between the group and all customers and partners, 6) use and training in information systems field, 7) the self-organization as a whole technical and IT group, and 8) the adding of daily experience.

The operations of the IT company are moving around three strategically selected axes that seek to meet the needs of the local market, in both the private and public sectors: system integration, service integration, and software integration, see Fig. 3.1. Also, the IT company is proud for its operations since 1998 and it states in its official web site that among of its most important achievements are:

- The implementation of a comprehensive system of organization and quality
- The creation of four “brick and built” stores and one on line store.
- The obtaining of a group of 30 partners with a high level of expertise.
- The creation of dozens of new products and software.
- The replacement and warranty for approximately 3,000 materials.
- The construction and installation of over 8,000 computers and finding of solutions for homes and businesses throughout Greece.
- It has over 10,000 new members in their online store.
It has provided customer service for about 25,000 customers in the region of Thrace and for 7,000 customers around the world electronically.

- It did over 35,000 technical works.
- It managed of over 50,000 cases to cover the requirements of their customers.
- Its employees have been working over 350,000 hours with over 43,000 days.
- It gave answers to more than 500,000 phone calls.
- Its web page received over 4,000,000 visitors and 30,000,000 readings.

Strategically Axes

Figure 3.1: Strategically selected axes for the operations of the IT company.

3.3 Research Strategy

There is adopted a qualitative methodology for the research with the conduction of semi-structured interviews (Creswell, 2009). An interview guide was formulated and it contained open and closed questions. The next step was the arrangement of interviews with the IS managers and the employees of the IT company for the collection of data, and the step after was the analysis of data, see Appendix D for a presentation of the research process. According to Yin (2003, in Baxter and Jack, 2008) this research is exploratory because it tries to identify in practice the affection of the behavior of the employees to their awareness to the company’s IS issues and ISP, see Fig. 3.2. Denzin and Lincoln (1994) present Stake’s arguments about case studies and stress that the
case has a second role for the research. The POST™ framework together with PEST analysis has been used as the basis for the conduction of the study in the IT company and the provision of the final results. The six psychological constructs of the framework consisted the six categories for more research, and every category was examined in order to formulate questions that would be in the position to identify the parameters that define the affection of every psychological construct to the behavior of the employees who adopt ISA or not.

Before the development of the interview guide the researcher read the existing literature about how the behavior influences the final decision of the end users to adopt ISA, see Appendix B. More specifically it was tried to be identified the theoretical background behind every psychological construct of POST™ framework, so as to understand why the individuals behave in some way or another. The first trial of the formulation of the interview guide was after reading the relative theory about the connection of the psychology of the end users with ISA. The questions were based on the subjective opinion of the researcher about how it was possible to understand the “why” of adoption of ISA or not by the employees. The task was on the one hand to develop general questions that would search about the individuals’ opinions about IS, and on the other hand the task was to identify if the employees adopt ISA or not and which psychological constructs contribute to such behavior. With the formulated questions for every psychological construct could be examined if the individuals: 1) have a background knowledge about IS issues and ISP, 2) respect the IT company’s IS issues and ISP, and 3) adopt ISA or not and the reasons for such behavior. Furthermore there was an examination of the individuals’ opinions about how could the constructs be used by the IS managers of the IT company in order to motivate them and their working groups to respect the company’s ISP (i.e. with the development of ISMS).

The next step was to give the formulated interview guide to fellow students (with background knowledge to the IS field) and ask from them to give a feedback. The fellow students agreed to participate in the proceeding, provided that they would remain anonymous. After the feedback of the fellow students and after conversations about their opinions for the interview guide it was decided that the interview guide should not be revised, but the researcher should better explain in the interviews what is
IS and how can IS be related with the behavior of the employees (one of the fellow students said that it would be nice if the researcher referred to the stakeholders on which book are the questions based on). Then the interview guide was given to the supervisor of the thesis so as to approve it and give directions accordingly. The supervisor stated that the questions in the category of Personality are too “direct” and may make the interviewees feel uncomfortable, so it would be better to exclude this type of questions if there’s not a strong collaboration between the interviewer and the interviewees. The final step was to give the interview guide to the IS manager of the IT company in order to express his opinion about what make him to feel uncomfortable and also about what should be additional included in the interview guide or be changed. The IS manager of the IT company didn’t have a problem with the interview guide but he didn’t also make suggestions about how could this interview guide be further improved. If there was any additional feedback by the IS manager of the IT company, then the researcher would revise the interview guide after a discussion with the supervisor.

Stake (1995a) argues that data can be separated into several categories and then analyzed (see in Baxter and Jack, 2008, p.554). Furthermore, Baxter and Jack (2008) state that the researcher can use a framework as an anchor for the conduction of a research and for the analysis of the collected data, and there is an opportunity for the researcher to improve the framework’s theory depending on the final results. Relating to the units of analysis of the study, the first step was the categorization of data to the six psychological constructs of POST™ framework depending on the content of the questions, and the step after was their coding (Patton, 2002). After the analysis of the data of every category, then there was a second analysis of the outcomes of all the sub-units in order to investigate the whole picture of the researched area (Baxter and Jack, 2008).

While using the POST™ framework it could be discovered which employees of the IT company adopt ISA or not. Also it could be examined the reasons for adopting ISA or not and it could be searched if the employees that adopt ISA and the employees that don’t adopt ISA perform similar characteristics in their behaviors. The reason that guided the researcher to examine the similarity in the behavioral characteristics between the employees that adopt ISA and those that don’t, was the belief that the IS managers in the organizations should develop ISMSs separately for those that respect the company’s ISP and those that don’t respect them. Then the total ISMS of the company could be a conjunction of the other two ISMSs. An additional “filter” was used for the analysis of the outcomes of the measurement of ISA adoption level in the IT company. This “filter” was PEST analysis and helped to discover which of the outcomes resulted from the affection of the external political, economical, social and technology factors to the behavior of the employees. Furthermore PEST analysis helped to identify if the external factors were the only factors that influence the ISA adoption level in the IT company, and it helped also to examine how the external factors influence the operations of the IT company.

The final step of the research was the development of an ISMS that was based to the outcomes of the measurement of the ISA adoption level in the IT company. The developed ISMS planed to cultivate an ISA culture in the IT company while ensuring that all of its employees will start or will continue to respect its ISP. In addition there was a trial to enrich the background theory of POST™ framework with the suggestion
of manners for its use as a measurement tactic and with the suggestion of means for evaluation of its measurement results, see Fig. 3.3.

![Figure 3.3: Research strategy.](image)

### 3.4 Data Collection

The research questions guide the researcher’s plans for the collection of data (Stake, 1995b). Walsham (1995, 2006) states that theory can be used as a map for the conduction of the research and the collection of data, a map for the collection and analysis of data or it can be part of the outcomes of the research. Furthermore, Walsham (2006) argues that in the interpretive research field there’s a necessity for cooperation of the researchers with organizations in order to continue their work and attain their goals. The collection of data was based on the conduction of semi-structured interviews with the IS manager and the employees of an IT company, and it was tried to be identified in practice their ISA adoption level (i.e. exploratory research according Yin, 2003, in Baxter and Jack, 2008). An e-mail was sent to the IT company in order to request their cooperation for the conduction of the research and then there were planned interviews with the stakeholders (after the approval of the developed
interview guide for the research by the IS manager of the IT company. The head office of the IT company has a workforce of 15 people (11 employees, 1 IS manager, 1 company director, 1 assistant manager, 1 business-sales manager), and 8 of them agreed to participate in the study (7 employees and 1 IS manager).

Myers (1997, p.9) argues that there can be several methods for the collection of data in a qualitative research such as interviews, observation and archival research, and he stresses that published and unpublished documents, company reports, memos, letters, reports, email messages, faxes, newspaper articles, etc… can be used as sources in a written form. Stake (1995b) states that the interviews are tool of the researcher to understand the different realities of the case. On the one hand the reasons for the selection of the employees as stakeholders for the conduction of the interviews were to collect data about their ISA adoption level, about their willing to respect IS issues in general and the IT company’s ISP, and about the affection of the six psychological constructs of POST™ to their behavior. On the other hand the selection of the IS manager was decided because there was a need to be discovered: 1) if the IS manager of the IT company would acknowledge the importance of IS, 2) if the IS manager of the IT company was aware to IS issues and the ISP of the company, 3) the reasons that guided the IS manager of the IT company to adopt ISA or not, and 4) the measurements tactics and the ISMSs that had been applied by the IS manager of the IT company until the time of the interview.

An informed consent form was distributed to the stakeholders so as to get informed about the procedures of the research and about confidentiality issues (e.g. anonymity, record of the interviews, etc). The participants were requested to sign the informed consent form and to write on it their full name or their first name, see Appendix C. The interviews were based on an interview guide that contained open and closed questions. Despite the fact that the interview guide was based on the existing literature about how the behavior of the end users influences their ISA adoption level, the formulated questions were general in their nature and not “framework driven” (Baxter and Jack, 2008, p.553). None of the questions was developed to produce a certain answer and the stakeholders were allowed to talk about their feelings, beliefs, thoughts, etc…relating the IS field. The background theory was the tool to evaluate the meanings of the answers from the stakeholders and to understand their “reality” about the researched theme.

There was a planning schedule with the IS manager of the IT company about the conduction of the interviews. Each interview lasted approximately from 20 to 30 minutes, and the interviewers were allowed to discuss about any issue that they felt it was important to be referred. Also the researcher had the opportunity to ask additional questions (if needed) at the time of the interview. The collected data were stored by the researcher for further examination and after the complete of the study they could be destroyed.

3.5 Data Analysis

The analysis of data started after their collection with the method of semi-structured interviews (Creswell, 2009). The analysis of data is highly related with the type of the research (Baxter and Jack, 2008). The method that was decided to be followed was the thematic analysis and a generic approach was used for the coding of data (Lichtman, 2013). There wasn’t a necessity for use of qualitative data analysis software (QDAS),
as the developed data set wasn’t large (Patton, 2002). Walsham (2006) states that the researcher’s thought stills to be useful even if there’s use of QDAS, because she/he has the responsibility to select the themes for analysis. Mumford (2006, p.387) argues that in small-scale surveys the most important data may be acquired from the interviews with the stakeholders despite the fact that there will be also the need for use of some kind of statistical analysis.

A word processing program was used for the collection and the organization of data (Lichtman, 2013). The background theory of POST™ framework helped to the classification of data to six thematic categories. These categories were the six psychological constructs of the framework, because by following this type of categorization of data it could be identified more easily the relation between the performing behavior of the employees who adopt ISA or not with the psychological constructs that guide such behavior. The formulated interview guide contained questions that tried to identify the employees’ thoughts and the way that they understood the “reality” behind adopting ISA or not, but the answers of the stakeholders were examined independently to the category that the questions were located in the interview guide. The questions were located in the interview guide relating the answers that the researcher believed they would provide, but it was not obligatory that the answers of the stakeholders would be useful to provide information only for the category in which the question belonged. In every category was given a code number in order to help the researcher to distribute the identified data from the answers of the stakeholders.

The text data that were founded in the answers of the stakeholders were first highlighted and after that they were given a code relating the category that they belonged. A second coding system used to aggregate the data in subcategories in every category, because Layton (2005) presents many additional theories behind every psychological construct and it was important to define the theory – subcategory in which the data belonged. The subcategories helped to better understand the “why” behind every answer. As the data were categorized in the six categories and in their subcategories, then it started the analysis phase with the use of the background theory of POST framework and the comparison of the findings with the other relative theory presented in chapter 2 of the current study (Baxter and Jack, 2008). The target of the above procedure was to provide statements about the employees that were found to adopt ISA or not and after that to explain from where these statements rise. The first priority was to discover if the employees adopted ISA or not and then their classification in two categories. After the categorization of the employees in two categories (i.e. employees adopting ISA/employees that don’t adopt ISA) it was tried to be identified the reasons for adopting ISA or not, and to discover if the employees that adopt ISA perform similar characteristics in the behavior with the employees that don’t adopt ISA.

All the above procedure constitutes the first circle of analysis and it gave as an outcome the foundation of which employees of the IT company adopt ISA, which employees of the IT company don’t adopt ISA, and the discovering of the reasons of why the employees of both the two categories perform such behavior, see Fig. 3.4. The second circle of data analysis was the use of PEST analysis in order to examine which of the factors that contribute the final decision of the employees to adopt ISA or not are affected only by the external political, economical, social and technology
environment. Discovering the influence of the external PEST factors to the employees’ behaviors it could be researched if the employees would perform an opposite behavior if the external factors stopped to exist. Benbasat, Goldstein and Mead (1987, p.374) state that the research starts from objectives and questions, it continues with the assumptions and the design choices, the uncovering of specific data, and it ends with the results and the conclusions. The PEST analysis “filter” was critical for the study as the final results of the analysis phase helped for the development of an ISMS separately for each category of the employees and after that the conjunction of the two ISMSs into one.

3.6 Validity and Reliability

A. Validity

According to Ayiro (2012, p.36) the validity of a measurement tool concerns the measurement results which have to be related with the initial thought of the researcher of what she/he wished to measure. In addition, the Author (2012, p.37, 38) argues about the two forms of validity (i.e. the internal and the external) and its three types (i.e. the content validity, the criterion-related validity, and the construct validity). Creswell and Miller (2000, p.125) argue that the quantitative researchers accept the concept of validity in the way that is presented above (i.e. internal, external, etc…), but the qualitative researchers give focus on the people that interfere in the research in any way (i.e. participate, read, conduct, view). Also, Creswell and Miller (2000, p.126) present a framework that helps the researchers to access the validity of their study depending on the paradigm assumption that it belongs. Shenton (2004, p.64) stresses the division of the validity in internal and external, and presents in detail the Guba’s (1981) criteria for achieving trustworthiness in a qualitative research.
Internal Validity - Credibility, when the research instrument is used for the purpose that is constructed (Ayiro, 2012, p.37); (Shenton, 2004, p.64):

The internal validity of the research has been tried to be ensured by the following procedures: 1) random sampling (Shenton, 2004, p.65), the selection of the participants was random and it was tried to be included in the study both the employees and the managers of the IT company, 2) triangulation (Shenton, 2004, p.65), the formulated interview guide has been checked by the IS manager of the IT company, by the supervisor professor and by other fellow students so as to examine its relation with information security awareness, 3) peer scrutiny of the research project (Shenton, 2004, p.67), the outcomes of the analysis of data has been examined by the IS manager of the IT company, by the supervisor professor and by other fellow students so as to check their objectivity (Lichtman, 2013), 4) the outcomes of the analysis has been checked by the supervisor and fellow students in order to check if they are too “framework driven” (Baxter and Jack, 2008, p.553), 5) tactics to help ensure honesty in informants (Shenton, 2004, p.67), the participants of the study (i.e. stakeholders in the interviews) could stop their cooperation with the researcher and leave the study any time they wanted, 7) thick description (Shenton, 2004, p.69); Creswell and Miller (2000, p.127), it has been tried to be given by the researcher a rich explanation of all of the research procedures.

External Validity - Transferability, when the results can be generalized (Ayiro, 2012, p.37); (Shenton, 2004, p.69):

The external validity of the research has been tried to be ensured by the following procedures: 1) There are clear statements by the researcher that: a) the outcomes of the analysis (about the reasons for adopting ISA or not) cannot be generalized to a bigger amount of population as the research took place in the head office of the IT company (the IT company has three branches in the biggest cities in the region of west Thrace in Greece) and among its 15 employees, only 8 employees agreed to participate in the study, b) the developed methodology for every step of the created ISMS cannot be used by the IT company (because of the low number of stakeholders), but the overall methodology (i.e. steps) of the presented ISMS can be used as a standard methodology for the organizations in general which want to increase the ISA adoption level of their employees, 2) the researcher provides information in detail about the IT company, the methods for the collection of data, the type (i.e. managers, employees) and the number of the stakeholders, and the time period for the interviews (Shenton, 2004).

B. Reliability

Golafshani (2003, p.604) relate reliability and validity with trustworthiness, rigor and quality, and stress that triangulation can be used as a concept in order to enhance the validity and reliability of the research method. Ayiro (2012, p.36) states that the reliability concerns the accuracy and precision of the measurement tactic that is going to be used. In addition, the Author (2012, p. 39) stresses that the reliability enhances the validity of the research although it does not provide a sufficient condition for validity. Shenton (2004, p.71) state that the reliability - dependability of the research depends on the ability of the researcher to construct the study in a manner that will provide the similar results every time is repeated in the same context, with the same methods and with the same participants.
The reliability of the research has been tried to be ensured by the following procedures: 1) the research design and its implementation, the research processes are explained in detail in order that the research can be repeated at any time and provide similar results (Shenton, 2004, p.71). 2) the operational detail of data gathering (Shenton, 2004, p.72), the researcher provided information in detail about the methods for the collection and analysis of data, 3) it has been used a computerized data base for the collection and organization of data (Baxter and Jack, 2008), 4) the interview guide was checked by the IS manager of the IT company so as to ensure that there wasn’t a mistake on the translation of the questions from the Greek language to the English language.

C. Risks

By the investigation of the possible risks for the research, it was discovered that: 1) there was a risk that the closed questions to the stakeholders will guide the answers of the stakeholders. So it was to include more open questions in the interviews so as to leave the stakeholders free to express their opinions, 2) the framework is related with the field of psychology research and there’s a risk that the thesis will be considered as irrelevant to the field of information security. So, there are clearly statements by the researcher to the stakeholders and to the readers of the thesis that it has been adjusted already existed theory about the human behavior in the psychological field to the field of IS and specifically to the field of ISA.

3.7 Ethical Considerations

A form of a written consent had been developed and distributed to the participants (before the conduction of the interviews) in order to inform them about the aim of the research, the procedures that were to be used, the ways for the conduction of the interviews, the ways for the store-examination-analysis of data and the type of questions that were to be used, see Appendix C. The role of the researcher was to handle all the procedures of the study relating the formulation of the questions for the interview guide, the conduction of the interviews, the collection and categorization of data, the analysis of data, and the provision of the final results. The researcher respected the privacy and confidentiality of the stakeholders while conducting the research and making the interviews, as only the researcher and the supervisor of the thesis had access to the obtained data and no one else knew about the answers of the stakeholders (Creswell, 2009).

The interview guide that was given to the IS manager of the company contained questions both in the Greek and the English language, so as to give the IS manager the ability to examine if there was an alteration of their meaning in the translation process and if there was a question that didn’t respect the policies of the company. Also the interview guide didn’t contain questions about very personal security themes (e.g. security codes…etc…), but it contained personal questions about the motives, attitude, beliefs, personality, morals and ethics of the stakeholders. So there were considerations about the level that the researcher would respect the privacy of the individuals, as they were asked to reveal their internal thoughts and describe in a manner their behavior. Kenneth and Herman (2008, p.131) argue that the meaning of the privacy can be different not only between the Countries, but it can also be different between the individuals in the same Country. The authors also state that privacy is divided in four categories: physical, decisional, psychological, and informational and
in the IT field the informational privacy has four subcategories: consumer privacy, medical privacy, employee privacy, and location privacy. The informational privacy is about the privacy of the individuals’ personal information (e.g. information about the everyday life of the individuals, etc...), and as the restricted access theory stresses, having informational privacy is the right of the individuals to reveal the information they like to others (Kenneth and Herman, 2008, p.141-142). On the one hand the researcher asked his questions to the stakeholders in a trial to understand the reasons that influence their psychology, and in turn, their behavior to adopt ISA or not. But on the other hand there was a respect of the privacy of the individuals, as they were informed about their rights and that they could not answer to any question that they didn’t want to answer (for their personal reasons). Also the stakeholders were allowed to reveal the amount of the personal information they wanted and they were free to stop the discussion - interview at any time.

The research didn’t have as a focus to get access to classified information of the company and the researcher respected the information security policies of the company. The IS manager of the company was asked about the hours that are the most suitable for the company for the conduction of the interviews. Furthermore relating the timing and the duration of the interviews, they had been planed so as to be quick and they had been arranged at a time that didn’t bother the employees at their “free time” on coffee breaks. Also there was a respect of the anonymity of the company and the participants, and the stakeholders were asked if they agreed to be recorded at the time of the interview (Walsham, 2006).

3.8 Translation Process

The questions of the formulated interview guide were developed in the Greek language because all of the stakeholders were Greek citizen. Despite the fact that the English language can be used by the majority of Greek people (even for simple communication with others) and that it is mandatory for the Greek schools the English language learning, the researcher decided to use the Greek language. The reasons for choosing the Greek language for the formulation of the interview guide and the conduction of the interviews were: 1) to fasten the procedure of the interviews as there was limited time, 2) to make the interview procedure more friendly for the stakeholders as they gave their answers in their native language and could communicate with the researcher more easily, 3) to make the interview procedure better for the researcher as he could write more easily the answers of the stakeholders (when needed) and ask additional questions without to think how to translate them in order not to lose their meaning, and 4) to make the analysis procedure more easy for the researcher as he could better understand the meaning of the answers.

Before the conduction of the interviews the IS manager of the company checked the interview guide that would be used for every interview and that contained written questions both in the Greek and the English language. The reasons for giving the interview guide to the IS manager of the company were to give him the opportunity to examine if the formulated questions respected the ISP of the company and to control if there was an alteration in the meaning of the questions that were in the English language. Although that there wasn’t a feedback by the IS manager that stressed the need to change the interview guide for any reason, it was identified in the analysis process that there were some questions that could lose their meaning or have a
different meaning in the English language. The different meaning of the translated questions was a consequence of the use of tones in the Greek words. Even a phrase that it is in the Greek language can obtain a different meaning if there is a different tone in the way that the Greek words are written or pronounced (e.g. during the interviews). The questions that can lose their meaning as a consequence of the translation process can be:

- **Do you think that every employee needs to do only what is described in his/her job requirements or only what his/her supervisor told him/her to do?**

  This question seems to be a leading question that asks from the stakeholders to choose one of the two options: 1) every employee needs to do only what is described in her/his job requirements and 2) every employee needs to do only what her/his supervisor told her/him to do. But in the Greek language the question is highly depended on the use of tones and asks from the stakeholders to express their opinion about what do they think that it is right for an employee to do. The truth meaning of the question is that the question asks the stakeholders to tell if the employees need to do just their job (i.e. according to their duties and according to the directions of their supervisors), if the employees need to do their job (i.e. according to their duties and according to the directions of their supervisors) and try to do additional things by their own, if the employees don’t need to do anything because they are responsible for their actions and no one can tell them what to do, if the employees need to do what they believe it is right to do, etc…The point is that the stakeholders could give any answer they wanted in the Greek language and they didn’t have to decide among two or more answers.

- **Are you good at work? What do you believe that makes you work in this way?**

  This question seems to ask the stakeholder if she/he is good at work and the reasons for being good. In the Greek language when is someone asked if she/he is good at work then it means that if she/he is a good employee who is “right” to her/his obligations to the organization, to her/his supervisors and to her/his co-workers. But there is a possibility that the meaning of that question in the English language can be different. For example someone can think that the question asks if she/he is a good person at work (e.g. friendly).

- **Can you make a description of your personality?**

  For the Greek culture this is a typical question which means in simple words: “tell me something about yourself in general so as to understand what kind of person you are”. But it is not only a question of culture; it is an ethical issue whether you should ask an interviewee about her/his personality. Also, this question can obtain a different meaning in the English language as it can be treated as a question that tries to uncover the internal world of the stakeholders by a psychological perspective. In order to avoid the non respect of the privacy of the participants, the researcher informed the interviewees before and during the interviews that they could refuse to answer in any question they didn’t like, and they could stop the interview procedure and leave any time they wanted.

- **Do you like working in groups or alone?**
This question seems to lead the stakeholders to decide if they want to work in groups or if they want to work alone. But there are employees that both enjoy to work alone and in groups. The properly use of tones in the Greek language (when asking the question) gives the opportunity to the stakeholders to provide any answer they like.

Do you think that the implementation of information security rules must not be applied if it does not serve the needs of the group (e.g. delay at work) or should we judge from the case before we act?

The above question can be considered as a leading question by the reader of the interview guide, but this is also a consequence of the translation process. The researcher gave this short meaning to the question in his trial to be more specific to the answers that the IS managers have to discover when asking the question. When the above question was used in the Greek language then the stakeholders were asked to argue about the properly implementation of the IS rules. The paradigms (i.e. must not be applied if it does not serve the needs of the group or should we judge from the case before we act) were used as examples while asking additional questions when the stakeholders provided answers to the question by a managerial perspective. So the aim of the additional questions was to find out which were the stakeholders’ opinions about the implementation of the ISP relative their ethics.

Knowing the dangers that exist in information security, do you believe that it would be unethical not to train properly your company’s employees?

It can be stated that the stakeholders are forced by the above question to provide a positive answer about the training of the employees so as to avoid to be considered as unethical persons. But this is also a consequence of the translation process, as while using the Greek language the stakeholders understood that they have to judge the non training of the employees from an ethical point of view.

All of the collected data were in the Greek language and they were translated after their analysis and the production of the final results. Nielsen, Mathiassen, and Newell (2014, p.182) state about the negative effects of the insufficient translation process for the IT usage. So it was tried to give the entire meaning of the final results when they were translated to the English language. Also before the translation process the researcher tried to take into consideration possible cultural differences between Greece and the other Countries so as to provide the meaning of the analyzed data in an objective way (Loogus, 2012). Finally it was tried to be given the entire meaning of the informed consent form that was given to the stakeholders, when it was translated from the Greek language to the English language.
Chapter 4: Results

In this chapter are presented the empirical findings from the study in the IT company. Then the findings are linked to the development of an ISMS for the IT company, and it is suggested a nine step procedure for the development of ISMSs which will ensure that all the employees of the organizations will adopt ISA. The chapter ends with the refinement of the POST™ framework.

4.1 Empirical Findings

The themes that emerged out of the thematic analysis are presented in Table 4.1. The following themes were examined separately according to the interviews of the stakeholders and it was tried to be identified: 1) if the employees adopted ISA or not, 2) which are the reasons for not adopting ISA, 3) if those that adopted ISA presented similarities to their behaviors with those that didn’t adopt ISA and which was the reasons for such behavior. A PEST analysis was conducted after the thematic analysis in order to examine the influence of the external political, economical, social and technology environment to the operations of the IT company and to the behavior of its employees.

Table 4.1: Themes of the analysis

<table>
<thead>
<tr>
<th>Number of theme</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theme 1</td>
<td>Motivation</td>
</tr>
<tr>
<td>Theme 2</td>
<td>Attitude</td>
</tr>
<tr>
<td>Theme 3</td>
<td>Beliefs</td>
</tr>
<tr>
<td>Theme 4</td>
<td>Personality</td>
</tr>
<tr>
<td>Theme 5</td>
<td>Morals</td>
</tr>
<tr>
<td>Theme 6</td>
<td>Ethics</td>
</tr>
</tbody>
</table>

After the collection of data from the conduction of 8 interviews with 7 employees and 1 IS manager, their thematic analysis and the PEST analysis, it was found that all of the stakeholders adopt ISA and they respect the most of the company’s ISP (and the IS issues in general). The problem was that all of them were found also to present similarities in their behavior with the behavior of the employees that don’t adopt ISA. More specifically it was discovered that despite there is a great interest about the
company’s ISP, in some situations the employees seem that they have not internalized the meaning of some ISP. The consequences of the inability of the employees to internalize some of the IT company’s ISP is the appearance of deviant behavior (from some of them), and the fear of the IS manager that the employees may not adopt ISA in future. The context of the divergent behavior and the reasons that guide the employees that adopt ISA to behave in the way they behave is presented in the paragraphs below. Also in the following paragraphs is presented the affection of the external environmental factors to the behavior of the employees.

Motivation

Two-Factor theory and Equity theory

Some participants present dissatisfaction about their working environment. According to the Two-Factor theory (paragraph 2.3.1) the bad working environment can have as a result the bad working behavior of the employees. In the IS field the bad working behavior can lead to the non respect of the organization’s ISP. Participant A said:

"disappointment exists when not be heard on a subject"

This employee feels that her opinion isn’t always heard by her fellows and her supervisors, even if she is right on what she believes. This is a reason that can lead her to the non respect of the company’s ISP, as it makes her to lose the interest for her job. Another employee, participant B said:

"there is lack of understanding in the job environment…and…repeats “

Also, participant C, said:

"there is... reluctance for work sometimes...sometimes I’m tired and feel disappointed with my job……”

Participants B and C feel also disappointed with their job because the employees don’t cooperate with each other and don’t understand each other. Also participant B founds himself to do the same things many times and this makes him to be tired. Participant C argues about the reluctance of his fellows to work sometimes, so he feels unhappy with his job because he cannot cooperate with the other employees (Two-Factor theory) and he is unsatisfied with the fact that he has to do more work (Equity theory). Another employee that is disappointed with the working environment of the IT company is participant D, who says:

"...buzz and intensity....I’m not completely satisfied with my job...feel disappointed with some things...”

For participant D the working environment of the IT company needs to be more quite and the employees have to cooperate in peace. The existing environment is too noisy and there’s intensity in the relations between the employees.

Need theory
The use of the Need theory helped to identify some factors that can influence the final decision of the employees to respect the company’s ISP now and in the future. Participant A, said:

“we receive a salary and therefore we must be correct to our obligations”

So this employee feels that she must “return” the salary she gets with being right to her obligations (i.e. money for food, water, etc, physiological needs). The problem with this opinion is that it is doubtful of which will be the employee’s attitude if there’s a delay to her payment or a reduction to her salary. Participant A admitted that she doesn’t respect all of the company’s ISP, as she said:

“I would give my computer security code to colleagues to quicken their job ... without a second thought”

The social needs of the participant make her not to respect the ISP which stress that the personal code of every employee has to be kept secret from the other employees. Participant F seems to give also great interest for the social needs, and he expresses his disappointment for some behaviors in his working environment.

“...there has to be more understanding to personal problems...”,
Participant F

The ego needs and the self-actualization need are in the top levels of the pyramid of Maslow (paragraph 2.3.1). Participant D, said:

“I dream a steady and upward career in the field I studied”

It is not easy for an employee in Greece to find a job that will be in the field that she/he studied, but the organization can locate the employees to places of their interest or to give them duties that are close to their field of studies. The comment of participant D reveals that he hasn’t duties that are close to his interests, and that makes him to be dissatisfied with his job.

Expectancy theory - Operant Model

Some employees revealed their perceptions about how restrict should the company’s ISP be (Expectancy theory) and others argued that there has to be a positive or negative reinforcement (Operant Model). Participant D, said:

“the reward or punishment should be made more efficient and they have to give more importance to IS”

Also participant G, said:

“...there have to be sanctions and positive feedback....”
The employees believe that the IS manager of the company need to reward the employees that respect the company’s ISP and they need to punish the employees that don’t respect the company’s ISP. The above comments reveal that there is a disappointment of the employees, as they believe that the company should give more importance to the IS field. It is believed by other employees that the company should give motives to its employees, so as to respect its ISP. Participant E, said:

“my salary has been reduced.....financial bonus would help to make all the employees to respect the company’s ISP ...”

For participant E the positive reinforcement is something that would make her to be more compliant with the company’s ISP. Also participant H, said:

“...I don’t like to see people with misery about the situation in Greece...”

So the arguments of participant E become more reliable as we understand that the economical themes concern a large amount of the employees. Participant F, said:

“...they must demand but they have to give also...”

The above comment reveals the beliefs of the participant when he was asked about what else should be done in the company. Participant F believes that if the employees take awards then they will be more efficient in their duties, so they will respect more the company’s ISP.

**Attitude**

It is important to discover when examining the psychological construct of attitude why the employees respect the ISP of the company. The affective component of attitude is related with the emotions of the individuals when the read, hear and talk about the company’s ISP or when they read and hear the IS messages (Layton, 2005). Participant A, said:

“feeling about norms? The obligation to follow them”

This comment was the answer to the question about what does she feel when she reads the IS norms. All the answers from the other stakeholders were neutral but participant A argues that her feelings are expressed as obligation and in the question if there’s a fear behind obligation she answered positive. Johnston and Warkentin (2010) state that in some cases the fear is negative for making the employees to respect the company’s ISP, as they may adopt an opposite behavior to avoid fear.

The other findings on this theme were related with the behavioral component of attitude (paragraph 2.3.2). Participant B, said:

“I apply the information security norms depending on the situation”

In the same direction participant C, said
“I don’t apply all the information security norms under any circumstances”

Participant E, said

“I don’t apply all the information security norms when there’s a lot of work to do”

Both participants B, C and E adopt an attitude that is affected from their behaviors. These employees decide not to respect the IS norms when they feel that they don’t have time to do it. Also according to the background theory of POST™ framework the participants belong to the category of the employees that want to do their job fast, so they will remove all the steps that delay them (Layton, 2005).

Also, participant F, said

“I don’t apply all the information security norms for simple things such as my personal code for the pc”

This comment reveals that the employee hasn’t internalized the meaning of how important is to keep secret the personal code of your personal pc, and this is the reason for adopting such an attitude – behavior.

Beliefs

In this theme are presented the findings that were identified related the beliefs of the employees about the ISP of their company and the IS issues in general. The beliefs of the stakeholders reveal the reasons for adopting a certain behavior and examining them gives the IS manager of the company the opportunity to better understand of what has to be improved.

“There must be rigour but not to an excessive degree because that makes us fear and then we cannot work in peace, Participant A”

Participant A argues that the fear has negative consequences to the working environment in the IT company. She also says that it is positive to make the employees to feel that they will be punished if they don’t respect the ISP of the company but they must not feel unsafe all the time. Also participant D, said

“... the right punishment for those that don’t respect the company’s information security policies is reprimand or comment.... I would give much more notice to IS issues if there was a punishment or reward...”

Same as the participant A, the participant D agrees that the sanctions and the positive feedbacks would make him to better respect the company’s ISP. The participant believes that there has to be motives which will make the employees to adopt ISA, but he stresses that the employees don’t need to fear that they will be fired if they make a mistake. In an additional question about what would happen if the
employees made mistakes all the time, the participant D said that they have to be fired because they will not respect their supervisors and their good willing.

“...the ISP of the company has to be more restrict....”,
Participant G

For participant G, the ISP of the policies of the IT company have to be more restrict because he feels that this will make all the employees to better respect them. The participant doesn’t believe that the punishment of the employees is the better ISMS in order to make them to adopt ISA. The employee bases his answer on the feeling that the ISP of the company don’t give the employees to understand that they have to respect all the IS issues. In the same direction, participant H, said:

“....the company’s ISP have to renewed...”

Also, participant D, said:

“the information security norms of my company are inadequate”

Both the participants H and D argue that they are not satisfied with the existing form of the company’s ISP. They believe that the existing ISP are inadequate in order to protect the company from threats in a rapidly evolving technological and social environment. Participant B, said:

“information Security is good, but it has to be applied”

With the above answer the participant expresses his opinion about IS. The participant stress the need for the appliance of the ISP in his company and the interest of the IS manager to examine that these ISP are followed by all of the employees.

Relating the ISTPs of the IT company, all of the employees answered that they have participated in ISTPs in the past. But participants D and C, said:

“....no ISTPs in the Company....”

Also, participant F, said:

“.... the ISTPs have to be more often....”

The newest employees of the company have not participated yet in an ISTP, and they are not satisfied with the fact that they’re not trained enough in the field of IS. Participant F, who is an employee that works for 6 years in the company, believes that the ISTPs positive affect the behavior of the employees. Furthermore, he believes that the IS manager of the IT company should arrange ISTPs more often.

**Personality**

**Trait-based Approach - Agreeableness**
The “Big Five” traits can help IS managers to identify the traits of personality that contribute to the building of the behavior of the employees and influence their final decision to respect or not the company’s ISP. Also, by the examination of the personality traits can be discovered the reasons that make the employees to perform a certain behavior. The agreeableness is the willing of the individuals to help, trust and understand the other people, and try to cooperate with them by making the things easy (paragraph 2.3.4). Participant A, said:

“I would give my computer security code to colleagues to quicken their job ... without a second thought..... I’m very careful towards myself and others... “

Also participants E and F, said:

“....I would give my personal pc code....”

And participant G, said:

“I give my code only when there is a true need for that...”

The willing of the above employees to cooperate with their fellows and to care about them or help them when there’s a need to do it, makes them not to respect the ISP of the IT company. More specifically, participants A, E, F and G seem to trust their fellows so much, so as to believe that the other employees won’t harm them or the company by revealing some of its classified information. In addition, the above participants enjoy to help the others and they prefer to risk by ignoring the ISP of the IT company (i.e. protection of the personal PC code), than feeling that they will be not liked by the others.

Despite that there are employees that care about their fellows, some employees feel different.

“there is lack of understanding in the job environment...” , Participant B

“...more understanding to personal problems...” , Participant F

Participants B and F complain in some manner for their working environment, as they feel that the other employees don’t give an understanding to their personal problems and many times there’s a lack of understanding between the employees in general. The feelings of the participants make them to feel disappointed with their working environment and this can influence their ISA adoption level (Layton, 2005).

Trait-based Approach – Introversion/Extroversion

The answer of participant B to the question which asked him if he wants to work alone or with a team was:

“I like both working alone and with a team”
All of the other employees answered that they want to work with a group, but participant B is the only employee who enjoys working in a group and alone. The desire of the employee to work alone reveals the introversion trait of his personality, which born concerns about the cooperation of this employee with his fellows and the IT company in general. On the other hand, participant F, said:

“sometime I like gossip...just for fun with fellows...”

Participant F was the only one who admitted that he likes gossip. This is an extroversion trait of his personality, which born concerns about the consequences of this social interacting (see Warkentin et al, 2011).

Trait-based Approach – Neuroticism

Participant A answered to the question which asked her if she has a moody character

“...yes and I try to calm and control it...”

The above answer reveals a higher level of neuroticism (emotional instability) and participant A admitted (as it is presented in the paragraphs above) that she doesn’t respect all the ISP of the company in any circumstances. Layton (2005) argues about the influence of the higher level of neuroticism to the final decision of the employees for not adopting ISA, so the above trait of the participant’s personality can be considered as a reason for her behavior.

Trait-based Approach – Conscientiousness

“..there is reluctance to work sometimes...”,
Participant C

Participant C expresses his disappointment about the unwilling of some employees to work. This is a conscientiousness trait of their personality which presents the continuum of their characteristics that make them to be careless, not helpful and less responsible (Layton, 2005).

Motive-based Approach

“I dream to attain economical benefits...”,
Participant C

Participant C answered that he wants economical benefits to the question which asked him about what does he dream to attain in his job. The IT company doesn’t award with financial bonus the employees that adopt ISA, and this can influence their willing to respect the company’s ISP in future.

Morals

While examining the thematic category of morals, it was discovered that the majority of the employees seem to present care characteristics about their employees but not in an intensive tense. The answers of three employees ( for the question, You trust your colleagues so much, that you don’t believe that they will ever reveal any critical
information of the company that you are supposed to handle?) present on the one hand an intensive tense of trust for the others, and on the other hand lack of trust. Participant A and F, said

“I don’t trust them now but the relations between the employees get better with the pass of time...”, Participant A

“I trust my fellows, but not all of them, Participant F

Also participant C, said:

“I trust my fellows very much...”

The above answers of the participants reveal their postconventional moral development and the way that they judge the morality of others according to their own values of morality (conscience and universal principles, paragraph 2.3.5). The participants A and F believe that their fellows (or some of them) don’t worth their trust and this is the way they judge their fellows’ morality. Despite the fact that in the IS field it is preferred not to trust anyone, the inexistence of trust in general between the employees may have the opposite results (i.e. bad working environment, Layton, 2005). Participants A and F gave focus with their answers to the fact that they don’t trust their fellows in general and they continued (with their answers to additional questions), that maybe in future they will attain to have good relations with the other employees and then they will trust them. On the other hand, participant C admits that he doesn’t respect the ISP of IT company, and the reason for such behavior is his too much trust to his fellows.

Ethics

The majority of the employees supports the deontological theories and believe that they must behave in a manner that serves the common good. Participants A, B, E, F answered to the question that asked about why should we not steal:

“.. it is not right to deceive others...”, Participant A

“.. it is not right to steal...”, Participants B, E, F

On the other hand, participant D answered to the same question:

“we should not steal because this is a criminal offense...”

According to the opinion of participant D the people should not steal because the law doesn’t allow them to do it. There is presented an absence of deontological values and the occurrence of utilitarianism ethics. The laws which are based on ethical values have been built along to the centuries relating what is right for the greatest number of people in the country in which the law is applied (the central religion of every country plays the greatest role to that direction). In contrast the answer of participant D for the question “Do you think that the implementation of information security rules must not
“be applied if it does not serve the needs of the group (e.g. delay at work) or should we judge from the case before we act?” was:

“….judge from the case before we act...”

Participant D says that in some cases the ISP have to be applied although they won’t serve the needs of the group (i.e. the greatest number of the employees). But this opinion differs from his beliefs about why not to steal, so the participant D acts at last according to his personal ethical values of what is right to be done or not (Contractarian Theory) and depending from the case (Act-Utilitarianism).

Relating to the monitoring of the employees in their job, participant A, said:

“yes to monitoring because this is a way to protect the innocent employees and there is a better control from the supervisors”

Also participant H, said:

“yes to monitoring if this won’t make more difficult the working conditions of the employees and their supervisors look all the time what they do…”

The participants A and H believe that it right to monitor the employees while they’re working, but only if this happens for the common good of the employees. Although their approach to the issue is from a deontological point of view, they are the only employees that stress the need for monitoring in the IT company.

PEST Analysis

A Pest analysis “filter” was used after the measurement of the ISA adoption level in the IT company. The thematic analysis and the use of the background theory of POST™ framework helped to identify if the employees of the IT company had internalized the meaning of IS (Siponen, 2000) and if they had adopted ISA or not. Also after the measurement of the ISA adoption level in the IT company, it could be indentified the reasons that guide the decisions of the employees for not adopting ISA, and it could be examined if the employees that adopt ISA perform similar characteristics in their behavior with the employees that don’t adopt ISA. An analysis of the external environmental factors supports the produce of the final outcomes, as it helps to understand the level of the affection of the external political, economy, social and technology factors to the behavior of the individuals and the operations of the IT company.

After the thematic analysis was founded that all of the employees of the IT company adopt ISA, but they perform similar characteristics in their behavior with the type of behavior that is described in the literature (Layton, 2005) as representative for the employees that don’t adopt ISA, see Table 4.2.
Table 4.2: Measurement Findings

<table>
<thead>
<tr>
<th>PARTICIPANT</th>
<th>THEME</th>
<th>REASONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Motivation</td>
<td>Two-Factor theory</td>
</tr>
<tr>
<td>B</td>
<td>Motivation</td>
<td>Two-Factor theory</td>
</tr>
<tr>
<td>C</td>
<td>Motivation</td>
<td>Two-Factor theory</td>
</tr>
<tr>
<td>C</td>
<td>Motivation</td>
<td>Equity theory</td>
</tr>
<tr>
<td>D</td>
<td>Motivation</td>
<td>Two-Factor theory</td>
</tr>
<tr>
<td>A</td>
<td>Motivation</td>
<td>Need theory (physiological needs, social needs)</td>
</tr>
<tr>
<td>F</td>
<td>Motivation</td>
<td>Need theory (social needs)</td>
</tr>
<tr>
<td>D</td>
<td>Motivation</td>
<td>Need theory (ego needs, self-actualization)</td>
</tr>
<tr>
<td>D</td>
<td>Motivation</td>
<td>Expectancy theory</td>
</tr>
<tr>
<td>G</td>
<td>Motivation</td>
<td>Expectancy theory</td>
</tr>
<tr>
<td>E</td>
<td>Motivation</td>
<td>Operant Model</td>
</tr>
<tr>
<td>H</td>
<td>Motivation</td>
<td>Two-Factor theory</td>
</tr>
<tr>
<td>F</td>
<td>Motivation</td>
<td>Operant Model</td>
</tr>
<tr>
<td>A</td>
<td>Attitude</td>
<td>Affective component</td>
</tr>
<tr>
<td>B</td>
<td>Attitude</td>
<td>Behavioral component</td>
</tr>
<tr>
<td>C</td>
<td>Attitude</td>
<td>Behavioral component</td>
</tr>
<tr>
<td>E</td>
<td>Attitude</td>
<td>Behavioral component</td>
</tr>
<tr>
<td>F</td>
<td>Attitude</td>
<td>Behavioral component</td>
</tr>
<tr>
<td>A</td>
<td>Beliefs</td>
<td>No fear/ Punishment or reward</td>
</tr>
<tr>
<td>D</td>
<td>Beliefs</td>
<td>Punishment or reward/ No fear</td>
</tr>
<tr>
<td>G</td>
<td>Beliefs</td>
<td>More restrict ISP</td>
</tr>
<tr>
<td>H</td>
<td>Beliefs</td>
<td>Renew the ISP</td>
</tr>
<tr>
<td>D</td>
<td>Beliefs</td>
<td>ISP are inadequate</td>
</tr>
<tr>
<td>B</td>
<td>Beliefs</td>
<td>Appliance of the ISP in the company</td>
</tr>
<tr>
<td>D</td>
<td>Beliefs</td>
<td>No ISTPs</td>
</tr>
<tr>
<td>C</td>
<td>Beliefs</td>
<td>No ISTPs</td>
</tr>
<tr>
<td>F</td>
<td>Beliefs</td>
<td>ISTPs more often</td>
</tr>
<tr>
<td>A</td>
<td>Personality</td>
<td>Agreeableness</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>E</td>
<td>Personality</td>
<td>Agreeableness</td>
</tr>
<tr>
<td>F</td>
<td>Personality</td>
<td>Agreeableness</td>
</tr>
<tr>
<td>G</td>
<td>Personality</td>
<td>Agreeableness</td>
</tr>
<tr>
<td>B</td>
<td>Personality</td>
<td>Introversion</td>
</tr>
<tr>
<td>F</td>
<td>Personality</td>
<td>Extroversion</td>
</tr>
<tr>
<td>A</td>
<td>Personality</td>
<td>Neuroticism</td>
</tr>
<tr>
<td>C</td>
<td>Personality</td>
<td>Conscientiousness</td>
</tr>
<tr>
<td>C</td>
<td>Personality</td>
<td>Motives</td>
</tr>
<tr>
<td>A</td>
<td>Morals</td>
<td>Lack of trust</td>
</tr>
<tr>
<td>F</td>
<td>Morals</td>
<td>Lack of trust</td>
</tr>
<tr>
<td>C</td>
<td>Morals</td>
<td>Intensive tense of trust</td>
</tr>
<tr>
<td>A,B,C,E,F,G,H</td>
<td>Ethics</td>
<td>Deontological</td>
</tr>
<tr>
<td>D</td>
<td>Ethics</td>
<td>Utilitarianism / Contractarian Theory</td>
</tr>
<tr>
<td>A</td>
<td>Ethics</td>
<td>Right to monitor</td>
</tr>
<tr>
<td>H</td>
<td>Ethics</td>
<td>Right to monitor</td>
</tr>
</tbody>
</table>

- **Political (together with the legal factors):**

Greece is a country of southeastern Europe and has a population of approximately 10,000,000 people. Greece is under financial crisis since 2009 and has entered in a black paged history period of a political, financial and cultural instability. The political party of socialists was the last political party that governed the country until 2012, while being self-dependence in the Greek parliament. In the period from 2012 to 2015, Greece has conducted national elections for three times and no political party governed without the cooperation of another political party. The political situation was so unstable, that after the national election of the country in 2012 there wasn’t cooperation between the political parties, and a functional government was hired until the next national election. No political ideology exists as the previous government was formulated by rightist-socialist-nationalist political parties at first and then by rightist-socialist-lefty political parties, when the nationalists decided that they didn’t want to cooperate anymore with the other political parties. The current government has been formulated by the cooperation of a lefty with a rightist (very close in its ideology with the nationalist political parties) political party. The unstable political environment of Greece is depicted also by the fact that since 2012 there is a political party in the Greek parliament (third in votes after the last national elections) that builds its political ideology in Nazism.

After the economical crisis of Greece and under the pressure of the EU partners, there have been revealed by the social media many cases of political corruption (e.g.
commission from arming programs, etc…). The citizen of Greece have lost their trust to politicians and the “tense” relationship with the Greek’s traditional political partners of West increases the fears for exit of the country from EU. Another problematic situation after the financial crisis is the conjunction of the public services. The public services have concentrated to the biggest cities of every region and it is now much more difficult for the citizen to be well serviced, as all the procedures are more time spending (i.e. more people and more bureaucracy).

According to the experts of the operational business market of Greece, the absence of governmental programs for the advance of the business market, the deficient governmental politic plans and the existing legislation incommod the advance of the enterprises (Ioannidis, 2013). The following reformulations are needed by the political scene for the economic and social reconstruction of Greece: 1) faster and more efficient justice, 2) stable, simple and predictable tax framework, 3) sustainable and equitable pension system, 4) combating youth unemployment, 5) greater flexibility of the education system, with continuous review its upgrade, 6) promoting research and commercialization of innovations, 7) suppression of corruption bureaucracy and overregulation, 8) acceleration and transparency in public procurement, and 9) strengthening the internationalization of Greek economy (IOBE, 2014, p.5-6). Gramelis and Pedioti (2014) state in their report for Small Business Act (SBA) that the main problems of the political and legal environment are:

**Legislation:** The enterprises are forced to pay high taxes during the economical crisis and the value added tax (VAT) is among the highest comparing with the other countries of Europe. The continuing reformulations of the tax system, the absence of tax exemptions and the tax-free threshold constituted to the growing problems of businessmen. Furthermore the abolition of tax-free accounts of enterprises reserves from January 1, 2015 makes businesses struggle to survive.

**Competition:** There is a great concern about the competition rules in the Greek market place. The increase in illegal trade makes it difficult for legitimate businesses to survive, and the large differences in prices of goods and services between businesses results to the survival of the big enterprises and the bankrupt of the small.

**Bureaucracy:** The businesses establishment procedures are very complicated and time spending (please see additional, Athens chamber of commerce and industry, 2015). Also there aren’t centers that inform – advise – direct the businessmen about the bureaucratically procedures, and there is a problematic situation about the use of land in many locations of Greece.

**Extroversion:** A main problem for the economy of the country is its large trade deficit, and it is a result of the large amount of imports and the reduced number of exports.

The region of West Thrace is next to the borders between Greece and Turkey. After the war in Afghanistan and in Syria many people tried to survive and escape from their countries so as to find a better place to live. Greece is the “bridge” for those who want to enter Europe, so the country serves as a path to a better way of living for those that escaped from war. There is high amount of illegal immigration and despite the political moves of Greece and EU (e.g. frontex, etc…), the number of the illegal
immigrants in Greece hasn’t been reduced. The majority of the illegal immigrants enter to Greece through Turkey (i.e. West Thrace or Aegean Sea) and many of them decide to stay in Greece. Unfortunately many Greeks exploit the illegal immigrants and offer to them jobs with low salaries or in many cases without salaries (i.e. food and a bed to sleep). The consequences of the illegal immigration are that many Greeks remain unemployed (because they demand better salaries) and that the illegal immigrants send the money they save abroad (e.g. to their families).

The IT company is affected by all of the above political and legislation factors, as do its employees and its customers. Unless these factors stop to exist, the company cannot extend its operations. Also there is a possibility for the company to enter in a period of instability if the geopolitical factors that influence the Greek marketplace become worse. In addition the employees of the IT company are affected by the external political - legal factors (e.g. participant D dreams a career in the field he studied and participant H doesn’t like to see people with misery about the situation in Greece), but it is not presented a “negative” behavioral characteristic in the employees that adopt ISA that can be a result of this affection.

- Economic:

Some of the consequences of financial crisis in the economic field were the reducing of the employees’ salaries in the private and the public sector, the reducing of pensions and the increase of the prices of goods and services. This time period is a time for negotiations with the economical partners and investors in order to continue helping Greece. If there isn’t an agreement between the Greek government and its partners then the country will get into bankrupt or it will be under controlled bankrupt with the exit of the euro coin and return to the old coin named drachma. Many of the citizens of Greece have transported their bank savings to other countries and try to save money so as to be ready if there’s a bankrupt.

According to the last economical research of IOBE (April 2015), the economical climate in Greece lies in the lowest level in comparison with the economical statements of the country for the last 16 Months. A main reason for this economical downturn is that there is also a decline of the customer trust, despite the fact that the customer trust index was in a high level after the national elections of Greece in February, 2015. The delay of agreement between Greece and its financial partners and creditors has as a result the absence of optimism to the customers and the organizations. The anticipations of consumers for the next 12 Months present aggravation of the economical ability of families, decline of the economical statement of Greece, increase of unemployment, inability of thrift for families, inability for larger shopping (e.g. furniture, electronic machines, etc..), rise of the prices of products and rise of the “economical depth” of families (IOBE, 2015, p.16-17).

The small and medium-sized enterprises (SMEs) are the basis of the Hellenic marketplace and they are financial supported from unofficial investors (e.g. kith and kin). Most of the Greek population choose to make business in order to survive and not for the exploitation of business opportunities (Ioannidis and Giotopoulos, 2015). The economical status of Greece remains in lower levels and there is a possibility for not recovering a higher rhythm of economical advance unless the Greek government makes reformations in the exports and imports of the country, cultivates direct
investments from businesses and investors that operate in the internal marketplace, and introduces factual capital in the economy from abroad (IOBE, 2014). According to the report of SBA, Fact Sheet for Greece the continuing economic downturn has brought disastrous results for SMEs and a continuously reduce both the value added and the number of workers in them. The SMEs have difficulties to access liquidity, to borrow funds from banks, to achieve lower supplier prices and to have different tax treatment (Gramelis and Pedioti, 2014).

As the IT company is a SME, it can be stated that it is in the same economical situation like the other SMEs in Greece at this period of time. It is positive that the company belongs to the SMEs that continued to operate since the beginning of the economical crisis, but the economical situation of the Country doesn’t help the company for its economical advance. The employees of the company have been affected by the external economical factors and their salaries have been reduced. So it can be stated that the behavior of some of the employees is highly influenced by the external economical factors. More specifically the behavioral characteristics of participants that talked about the reduction of their salaries and about the necessity of financial bonuses (participant E) are directly affected by the external economic factors.

- **Social (together with the ecology factors):**

As it has been stated above in the analysis of the political factors, the political scene of Greece has changed and the third political party in votes (in the last national elections) supports Nazism. There is an advance of the phenomena of racism not only to the immigrants from other countries, but also there is racism among the Greek citizen cause of their political beliefs. Another factor that influences the external social environment is the problematic health system. The insured and the uninsured citizens face a lot of problems with the existing health system such as bureaucracy, absence of doctors, lack of medicines, limited hospitals, limited rooms in hospitals, etc…Furthermore the indignation of citizen raises with phenomena of social exclusion such as the need of use of the internet (e.g. to make a return), because many of the oldest people cannot even use the computer and many people don’t have the ability to pay bills for internet connection.

The experts in the operational business market of Greece support that many companies have difficulties to enter the internal marketplace cause of the Greek culture and mentality (Ioannidis, 2013). According to the Global Entrepreneurship Monitor (GEM)/IOBE research program for 2012-2013 despite that there is a social acceptability and respect by the Greek society for those that succeed in businesses; the social media don’t choose to adduce cases of success in the enterprising field of operations. Also the results of GEM/IOBE research program for 2012-2013 reveal high performance in the Greeks’ skills, knowledge and experience to do businesses (Ioannidis and Giotopoulos, 2014). The GEM/IOBE research program for 2013-2014 presents that the unemployment level remains low because the Hellenic market keeps an introvert profile and it is based on small companies that don’t advance and don’t offer new jobs (Ioannidis and Giotopoulos, 2015).

Gramelis and Pedioti (2014) state in their report for Small Business Act (SBA) that the main problems of the social environment are:
**Education – training:** The level of the providing education and training in Greece (relating the establishment and advance of businesses) is very low comparing to other countries of EU. The programs that are in use cannot cover the needs of the businesses and there is no motivation for people to enter the programs.

**Insurance:** There are many problems to the insurance system of Greece and they are mainly caused by its economical crisis. Many enterprises bankrupted and deprived the imports of financial funds to the insurance system, and many enterprises are unable to pay insurance contributions. In addition, the insurance funds have liquidity difficulties because the insured do not pay their bills.

**Structures of counseling:** Although Greece is in economical crisis and the enterprises need to continue to operate in the marketplace, there is presented an absence of structures of counseling.

**Innovation:** The small enterprises present an inability to be innovative and use new or improved products and services, so it has to be created support structures for innovation for small businesses.

Despite the fact that the Greek government supports the protection of the environment, there is presented limited action by organized structures. Also the everyday picture of the cities reveals an absence of ecological consciousness by a high amount of the citizens.

The above external social factors affect the IT company and formulate the context in which is forced to operate. Also the external social factors that are related with the education-training present a direct affection to the company’s procedures (as it has to arrange ISTPs for a long period of time). So it can be stated that the external social factors about education/training, directly affect the behavioral characteristics of the employees that are disappointed about the ISTPs of the company (participants F, D and C).

**Technology:**

The outcomes of the GEM/IOBE research program for 2013-2014 present an increasing trend for the Greek businesses that want to use new technology. The use of new technological artifacts seems to constitute a solution for the survival of the enterprises in the financial crisis period (Ioannidis and Giotopoulos, 2015). Gramelis and Pedioti (2014) state in their report for Small Business Act (SBA) relating to the infrastructure of technology and communication, that there isn’t a wide use of the internet and e-invoicing services by the enterprises.

The economical inability of a large amount of the Greek citizens has as a consequence the limited use of the new technology. So the use of the new technology is supported only by those that have the economical strength to buy the technology, even if they are citizens or enterprises of Greece. Also there are presented many problems to the organizations that try to built their operations with the use of new technological artifacts (when their customers need to use new technological artifacts also) because they will have a limited number of customers in the internal market place.
The IT company needs to use new technology by its nature, and it keeps to advance its infrastructure when needed. It is not presented an influence of the external technology factors to the behavior of the employees that adopt ISA. Below are presented the outcomes of PEST analysis, see Table 4.3.

Table 4.3: PEST analysis

<table>
<thead>
<tr>
<th>FACTOR</th>
<th>COMPANY(C)</th>
<th>EMPLOYEES(E)</th>
<th>DIRECT AFFECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>POLITICAL</td>
<td>C</td>
<td>E</td>
<td>YES</td>
</tr>
<tr>
<td>POLITICAL</td>
<td>E</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>ECONOMIC</td>
<td>C</td>
<td>E</td>
<td>YES</td>
</tr>
<tr>
<td>ECONOMIC (PARTICIPANT E)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOCIAL</td>
<td>C</td>
<td></td>
<td>YES</td>
</tr>
<tr>
<td>SOCIAL (EDUCATION/TRAINNNING)</td>
<td>E (PARTICIPANTS F, D, C)</td>
<td></td>
<td>YES</td>
</tr>
<tr>
<td>TECHNOLOGY</td>
<td>C</td>
<td></td>
<td>YES</td>
</tr>
<tr>
<td>TECHNOLOGY</td>
<td>E</td>
<td>NO</td>
<td></td>
</tr>
</tbody>
</table>

4.2 Linking Findings to ISMS

The head office of the IT company was selected as a representative sample for the purposes of this investigation and among its 15 employees, 8 employees agreed to participate in the study. Thus the measurement results don’t represent the whole picture of the IT company (relating its employees’ ISA adoption level) and the outcomes of the analysis (about the reasons for adopting ISA or not) cannot be generalized to a bigger amount of population. Although the outcomes of the measurement/analysis don’t reveal if all of the employees of the IT company adopt ISA or not and the reasons for performing such behavior, they are examined as being the only results for the purposes of the study. The developed methodology for every step of the created ISMS cannot be used by the IT company, as it is considered inadequate. But the overall methodology (i.e. steps) of the presented ISMS can be used as a standard methodology for the organizations in general, which want to increase the ISA adoption level of their employees.
The following picture illustrates the steps that are suggested for the creation of an IS climate in an organization, see Fig. 4.1. It is stressed that it is supported both the socio-organizational approach and the socio-technical approach for the development of the organizational IS strategies (Bulgurcu et al., 2010); (Warkentin et al., 2011); (Kajtazi, 2013). In addition the IS managers can ensure by following the steps of Fig. 4.1 that the employees of their organizations will adopt ISA and they will respect the company’s ISP. In the case of the IT company it is considered that all the process started from the seventh step, where there’s a measurement of the employees’ ISA adoption level and the production of the final results. So the next step for the IS manager of the IT company is to develop an ISMS according to the measurement findings, and the step after is to implement the created ISMS. As it can be noticed into the picture, the whole procedure starts from the beginning after the ninth step, and it continues until the results of the measurement of the employees’ ISA adoption level become completely positive (i.e. all the employees adopt ISA and they don’t present similar characteristics in their behaviors with the employees that don’t adopt ISA).

Figure 4.1: Steps of the ISMS.
Step 1: Preparation

This is the first step of the whole methodology, where the IS managers (in cooperation with the other managers of the organization) prepare the culture of their organizations, so as to succeed in creating an IS climate among the employees. The IS managers need to cultivate a culture which will try to develop a cooperation climate among the employees, and it will try to advance their satisfaction for their working environment. In this phase the IS managers have to take into consideration the personal needs and the desires of their employees, and cover them as much as possible. Also, the IS managers should inform the employees about IS and communicate its necessity for the safety of the organization (Ashenden, 2008).

For the case of the IT company the IS manager needs to improve the satisfaction of the employees for their working environment (in cooperation with the other managers of the organization) by the cultivation of a cooperation climate among the employees and by the deepening of the relations between them. The employees of the IT company need to trust and help each other, so the “unwilling behaviors” should be limited. There has to be more understanding to the personal problems of the employees, and the employees have to feel “safe” and that they have the opportunity to succeed into their carrier. Furthermore, the IT company should punish or remove those employees that are unable to compromise with the new situation.

As there’s “buzz and intensity” (participant D), the company should limit such phenomena by the advance of a peaceful working climate. In addition the employees of the IT company need to be prepared for the advance of a new IS climate, where all of the employees will respect the company’s ISP. Unfortunately, the economical situation of the company and the employees are affected by the external economic factors, but the company needs to examine the possibility of an increase to the salaries of its employees or the provision of financial bonus to its employees (e.g. financial bonus for the employees that work in a better way than the others).

Step 2: Develop /Renew the company's ISP - Rules

The IS managers have to develop in this step the ISP of the organization, after they examine which are the possible external and internal threats that might harm the organization and its operations (Vance, Lowry and Eggett, 2013). The ISP of the organization have to be based on the behavior of its employees, in order that the employees will adopt ISA and they will respect the ISP in any circumstances. When the IS managers return to this step after they’ve measured the ISA adoption level of their organization, then they need to renew the existing ISP so as to be in accordance with the measurement findings.

According to the measurement findings from the study in the IT company, there’ a necessity for a renewal of the company’s ISP. The new ISP need to be restrict, but they mustn’t make the employees to fear. The employees support the punishment for those that don’t respect the company’s ISP and the positive feedback for those that respect them. So the IS manager of the company has to create certain IS rules and these rules have to warn the employees about the punishment of those that won’t respect them. Also the IS manager should stress that the respect of the company’s ISP will have positive results to the carrier of the employees. In addition the IS manager has to take into consideration before the renewal of the company’s ISP, that in some
cases the employees were founded not to respect the ISP cause of their trust to the other employees, their underestimation of the necessity of some of the IS rules (e.g., protection of the personal pc code), and cause of their willing to do fast their job (i.e. don’t respect the ISP when they’re hurried). As the majority of the employees seem to support the deontological ethics, the IS manager should ensure that the ISP will be renewed from a deontological point of view (common good, etc…).

Step 3: Communication of the ISP

The communication of the developed/renewed ISP of the organization to its employees is very critical, as the employees have to be informed about the content of the ISP (Ashenden, 2008). The IS managers shouldn’t expect that the employees of the organization will read the developed/renewed ISP on their own. Even if the majority of the employees will read the ISP of the organization, the IS managers have to ensure that all of the employees will know what to do to protect their organization from possible threats. The communication of the developed/renewed ISP can be supported by the use of handbook notes, the use of media and the use of web. Same as the IS managers of the organizations, the IS manager of the IT company needs to communicate the renewed ISP to the employees and inform them about the punishments or awards for those that respect or don’t respect them.

Step 4: Implementing the ISP

The implementation of the developed/renewed ISP concerns their implementation to the structure and the culture of the organization. After the communication of the ISP they have to be applied by all of the employees. Also the employees need to adopt ISA and internalize the meaning of the importance to respect the organizational ISP. As the culture of an organization is important for the governance of behavioral information security and the sharing of IS knowledge (Flores, Antonsen, and Ekstedt, 2014, p.106), the organization has to cultivate employees’ behaviors that will be complaint with its ISP and will isolate behaviors that don’t adopt ISA. Furthermore, the developed/renewed ISP have to be implemented in the structure of the organization. The technology which is used and the infrastructure of the organizations have to be adjusted to the developed/renewed ISP, and there has to be used IS messages that will be located in every place and will inform the employees about the IS rules and the possible threats (e.g. “don’t reveal your personal pc code as you can harm yourself and the organization”). Also there has to be a control for the shared information across the value chain, and between the organization, its customers, and its stakeholders (Ashenden, 2008).

The IT company needs to implement the renewed ISP to its culture only, as according to the measurement findings the causes of not respecting the ISP are born from behavioral characteristics of the employees. The employees of the IT company have to adopt a new culture which will support the respect to the overall ISP, no matter if that behavior will result to the dissatisfaction of other employees or the delay of finishing the work that has to be done.

Step 5: Arrange ISTPs – Training

The IS managers of the organizations need to arrange ISTPs so as to educate the employees about the existing ISP of the organization. According to Abawajy (2014,
p.240-243) the delivery methods of ISTPs are: 1) conventional delivery methods (electronic-paper resources), 2) instructor-led delivery methods (expert-based approach), 3) online delivery methods (e-mail broadcasting, online synchronous and asynchronous discussion, information uploading, blogging, animation, and multimedia), 4) game-based delivery methods, 5) video-based delivery methods, and 6) simulation-based delivery methods. All of the employees have to be trained no matter if they have experience on the IS field or not, because the IS field is evolving and many times there are identified new threats for the organizations. The time period between the ISTPs has to be short (e.g. every three months) so as to make the employees to understand on the one hand the high interest of the organization for the IS, and on the other hand the time period should be short so as to make the employees to adopt ISA.

The IS manager of the IT company needs to arrange ISTPs so as to train the employees on the renewed ISP. The ISTPs should be often repeated, as some of the employees complained about the inexistence of ISTPs or their low frequency (participants F, D and C). Also the IS manager should give focus on reminding the employees that every IS rule is important and they have to respect it, and that it is their responsibility to protect themselves and their fellows from an information misuse.

The IT company is a SME and as it was found from the interviews, it has to train its employees in the IS field for a long period of time. Unfortunately the training in general in this period of time is directly affected by the external social environment of Greece (as it was found after PEST analysis). The phenomenon of the “non training” is a general social phenomenon for the employees in Greece for many reasons (e.g. lack of time, lack of interest, etc…), but the main reason for the inexistence of the training programs since the beginning of the financial crisis is that the SMEs don’t have the economic ability to conduct training programs.

Step 6: Supervision – Control

In this step the IS managers of the organizations (it is the same for the IS manager of the IT company) should control that all of the employees respect the ISP and they don’t perform a divergent behavior. The employees that will be found not to respect the ISP have to be punished and there has to be awards for the employees that adopt ISA. The sanctions have to be different in every case and the IS managers should take into consideration the action that causes the punishment and the behavior of the employee that has to be punished. The supervision of the employees in their working environment increases the possibilities to respect the ISP, but the IS managers need also to ensure that the employees will adopt ISA and they will internalize the meaning of the ISP (Layton, 2005). Vance, Lowry and Eggett, (2013, p.266) argue that the cultivation of accountability (as a mechanism and not a virtue) to the employees of an organization can reduce the ISP violations and advance the ISA, and stress that (2013, p.268) identifiability (i.e. being responsible for your actions), evaluation (i.e. assess of someone’s actions by other groups which have certain rules and beliefs) – monitoring (i.e. noticing what someone does), and social presence (social interactions) increase accountability.

Step 7: Measurement of ISA adoption level
Kritzinger and Smith (2008, p.228, 230) suggest the Information Security Retrieval and Awareness (ISRA) model and state that this model can increase the employees’ ISA adoption level. The ISRA model is consisted of three parts: 1) the ISRA dimensions (non-technical information security issues, IT authority levels and state-of-the-art information security documentation), 2) information security retrieval and awareness, and 3) measuring and monitoring. According to the Authors the measuring and monitoring can help the organizations to identify the current ISA adoption level of the employees and to monitor that the organizations follow the continuing developments in the IS field and are properly adjusted (Kritzinger and Smith, 2008). The IS managers of the organizations (it is the same for the IS manager of the IT company) should arrange short measurements so as to identify the ISA adoption level of their employees. The POST™ framework together with PEST analysis are suggested as a measurement tactic for the collection - analysis of data, but the final decision remains to be on the IS managers. The focus of this step is to make IS managers to understand if the employees of the organization adopt ISA or not and if the employees that adopt ISA perform similar characteristics in their behaviors with the employees that don’t adopt ISA. After that IS managers have to identify the reasons that the employees perform a divergent behavior.

Step 8: ISMS development

Information security management helps an organization to succeed in attaining its IS goals, so it contributes also to the overall advance of the organization (Ashenden, 2008). After the measurement of the ISA adoption level in the organization and the provision of the final outcomes, the IS managers need to develop ISMSs that will be adjusted in the behaviors of the employees. The IS managers have to identify the reasons that guide the employees to the non respect of the organizational ISP and IS rules, and after that they need to develop ISMSs that will try to make these reasons to disappear. The PEST analysis helps the IS managers to examine which of the reasons that influence the final decision of the employees to adopt ISA or not are directly affected from the external environment. So that will help them to examine also if their organization can do anything to deteriorate the influence of the external factors.

For the case of the IT company the IS manager needs to develop an ISMS that will be based on: 1) the increase of the satisfaction of the employees for their working environment, 2) the renew of the company’s ISP, 3) the provision of awards or sanctions for the employees that respect the company’s ISP/IS rules or not, 4) the arrangement of ISTPs, and 5) the internalization of the meaning of the company’s ISP by its employees, so as to adopt ISA without to perform similar characteristics in their behavior with the employees that don’t adopt ISA.

Step 9: ISMS implementation

The final step is the implementation of the developed ISMS. The IS managers of the organizations (it is the same for the IS manager of the IT company) need to start implementing the ISMS by following the steps from 1 to 6, see Fig. 4.1, while adjusting the actions that have to be done in every step according to the measurement results of step 7. The whole procedure needs to be repeated until the IS managers identify that all of the employees adopt ISA and they don’t perform similar characteristics in their behaviors with the employees that don’t adopt ISA. If the IS managers identify that all the employees adopt ISA, then they need to keep following
the sixth step (supervision – control) and they need to arrange short measures in order to examine if there are any changes.

4.3 POST™ Framework Refinement

In chapter 2 is presented the POST™ framework and its background theory. Layton (2005) introduced the framework in order to give the IS managers the ability to arrange short measures to identify the ISA adoption level of the employees of the organizations. The framework helps also the IS managers to identify the reasons that guide the final decision of the employees to adopt a certain behavior. The six psychological constructs of *motivation, attitude, personality, beliefs, ethics, and morals* are according to Layton (2005) the basic components of the behavior, which are related with the willing of the employees to adopt ISA or not. So the IS managers of the organizations can identify if the employees adopt ISA or not by examining the six psychological constructs of their behavior.

Although the POST™ framework can help the IS managers of the organizations to develop suitable measurement tactics so as to identify the employees’ ISA adoption level (and the reasons why they behave in the way they behave), it is presented a limited ability of the framework to distinct which of the factors that guide the final decision of the employees to adopt a certain behavior are directly affected by the external political, social, economic and technology factors. PEST analysis (please see chapter 2) can be used as a second filter for the analysis of data so as to examine if the external factors are the only factors that influence the employees’ behaviors, and if the organization can develop ISMSs so as to deteriorate the influence of these factors.

More specifically with the use of POST™ framework can be intetified which of the internal and the external factors influence the psychological constructs of the individuals’ behaviors. The amount of the influence of the internal and the external factors to the behaviors of the individuals is depeated also from the influence of every psychological construct to the other psychological constructs, and the influence of the formulated behavior (until the time of the affection of the internal and the external factors) to the psychological constructs. The final affection of the behavior of the individuals from the internal and the external factors can be very low if the individuals are in the position to deal with them. If the affection has as a consequence the non adoption of ISA, then the final decision is made again by the individuals. But in some situations there can be an extreme affection of the external factors and the individuals may have not the opportunity to "judge" before they adopt a certain behavior (e.g. war situations, financial bankrupt of a country, terrorist attaks, etc...).

This is the reason why PEST analysis is critical for the measurement of the ISA adoption level in an organization. With the use of PEST analysis it can be examined the influence of the external factors and then it can be identified if the individuals can act against those factors or they’re just "victims". In addition PEST analysis helps to discover the affection of the external factors to the organization and its operations. So, it will be examined if the organization can act against the external factors in order to deteriorate their affection or not. If the organizatitons can act against the external factors then there’s a possibility to deteriorate their influence to the employees by the development of ISMSs, but if the organizations cannot act against the external factors then the possibilities of the direct affection of these factors to the employees are increased.
After the conduction of the study in the IT company it was discovered that the economic and the social environment directly affects the company and some of the employees’ behaviors, see table 4.3. If there wasn’t a PEST analysis then there would have been developed an ISMS that would try to deteriorate the affection of these external factors in a different way than the developed ISMS in paragraph 4.2. The research findings about the affection of the external environment to the behavior of the employees stress the need for the refinement of the POST™ framework as theory and as a measurement tactic, see Fig. 4.2. On the one hand the refinement of the framework as theory can be with the implementation of PEST analysis as a basic additional theory which will support the background theory of the psychological constructs (i.e. like the theory of the OCB). Also the PEST analysis will give the opportunity for a better examination of the affection of the external political, economical, social and technology factors to the behaviors of the individuals. On the other hand the refinement of POST™ framework as a measurement tactic can be with the implementation of the PEST analysis as the second "filter" of analysis after the IS managers discover which employees of the organizations adopt ISA or not, and which employees adopt ISA but present similarities in their behavior with those that don’t adopt ISA. The use of PEST analysis will help the IS managers to understand which of the external factors directly affect the behavior of the employees and the operations of the organization.

![POST™ framework refinement](image-url)

Figure 4.2: POST™ framework refinement.
The POST™ framework can support the IS managers to develop measurement tactics in order to identify the ISA adoption level of the employees in their organizations (i.e. help for the development of questionnaires, help for the conduction of the interviews, etc…), see Fig. 4.2. Also the background theory of the framework can be used for the analysis of the collected data after the measurement of the employees’ ISA adoption level. After the analysis of the data the IS managers of the organizations will be in the position to identify: 1) which of the employees adopt ISA, 2) which of the employees don’t adopt ISA, 3) if the employees that adopt ISA perform similar characteristics in their behaviors with the employees that don’t adopt ISA. In addition the IS managers will identify the reasons that the employees of the organization choose to adopt a certain behavior (Layton, 2005). The PEST analysis is the second “filter” of the analysis process and helps to examine the affection of the external political, social, economic and technology environment to the behaviors of the employees that adopt ISA (and perform similar characteristics in their behaviors with the employees that don’t adopt ISA) or don’t adopt ISA. More specifically, with the use of PEST analysis it can be discovered if the reasons that guide the final decision of the employees to adopt a certain behavior are directly affected by external factors. In addition the IS managers after the conduction of a PEST analysis will identify the influence of the external factors to the operations of the organization and they will examine if the organization can “deal” with those factors (as there is a possibility that the employees that are affected by the PEST factors will adopt ISA when these factors stop to exist). The final outcomes of the measurement will present a clear picture of the employees’ ISA adoption level and will enhance the ability of the IS managers to understand why the employees of the organizations adopt ISA or not. Then the measurement findings can be used for the development of ISMSs that will try to increase the ISA adoption level of the organization.
Chapter 5: Discussion

In this chapter an in-depth discussion about the empirical findings and their importance for the thesis is presented, followed by a critical discussion about the theory that has been used for the conduction of the study. Finally some reflections from the Author are provided.

5.1 Discussion on the Empirical Findings

The results after the conduction of the study in the IT company present the ability of the POST™ framework (both as theory and as a measurement tactic) to distinguish the employees that adopt ISA from those that don’t adopt. Also the framework helped to discover if the employees performed similar characteristics in their behavior with the behavior of the employees that are described from the background theory as being those that don’t adopt ISA. The employees of the IT company were found to adopt ISA but to perform similar characteristics in their behavior with the behavior of employees that don’t adopt ISA. The use of the background theory of POST™ framework helped the researcher to identify the “why” of those behaviors, as on the one hand its background theory was used for the formulation of the interview guide for the conduction of the interviews, and on the other hand its background theory was used for the analysis of data (i.e. it was used so as to help the researcher to discover the reasons that the participants gave these answers to the formulated interview guide).

Supporting the statement about the need of the use of PEST analysis so as to discover the affection of the external environment to the behaviors of the employees, it was decided to be used the PEST analysis as a second “filter” for the analysis of data. The final results ensure the necessity of PEST analysis, as it was discovered that the behaviors of some employees of the IT company are directly affected by the external economic and the social environment. So the measurement tactic that is proposed is the use of POST™ framework for the collection and analysis of data and after that the use of PEST analysis. The research method for the collection of data can be qualitative, quantitative, and both qualitative and qualitative, as the selection of the research method depends on the amount of the sample, the ethics of every region (i.e. the importance that is given for the conducted researches), and most of all it depends on the preferences of the researcher (Creswell, 2009).

The outcomes of the measurement of the ISA adoption level in an organization (while using the measurement tactic which is described above) can be linked to the development of ISMSs, as they will present why the employees adopt ISA or not. Also the measurement findings will illustrate all the areas that need changes, so as to increase the satisfaction of the employees and their willing to respect the organizational ISP and IS rules. An ISMS of nine steps is proposed so as to help IS managers to develop an IS climate in their organization, where all of the employees will adopt ISA. These steps are: 1) preparation, 2) develop /renew the company's ISP – Rules, 3) communication of the ISP, 4) implementing the ISP, 5) arrange ISTPs – training, 6) supervision – control, 7) measurement of ISA adoption level, 8) ISMS development, and 9) ISMS implementation. After the final step the IS managers follow the steps from 1 to 6, and start to implement the ISMS while adjusting the actions that have to be done in every step to the measurement findings. The whole
procedure is repeated until the IS managers identify that all of the employees adopt ISA (i.e. in step 7).

A refinement of the POST™ framework is suggested, where the POST™ framework is used as a measurement tactic which tries to identify: which of the employees adopt ISA or not, if the employees that adopt ISA perform similar characteristics in their behaviors with the employees that don’t adopt ISA, and the reasons why individuals behave the way they behave. PEST analysis is the second “filter” which examines the affection of the external political, social, economic and technology environment to the behaviors of the employees that adopt ISA (and perform similar characteristics in their behaviors with the employees that don’t adopt ISA) or don’t adopt ISA. The goal of the framework remains to be the identification of the reasons that influence the employees to adopt a certain behavior.

5.2 Discussion on the Theory

This thesis supports both the socio-organizational approach and the socio-technical approach for the development of the organizational IS strategies (Bulgrucu et al, 2010); (Warkentin et al, 2011); (Kajtazi, 2013). It also supports the prescriptive model (Siponen, 2000); (Layton, 2005); (Webb et al, 2014) and stresses that the behavior of the end users is the factor that defines the ISA adoption level in an organization. According to Siponen (2000) the end users need to internalize the meaning of the ISP and norms in order to adopt ISA. In addition Layton (2005) argues that the internalization of the meaning of IS is depended on the behavior of the end users, which in turn is depended by their psychology. The author presents six psychological constructs (motivation, attitude, beliefs, personality, morals, and ethics) and stresses that these constructs influence the behavior of the end users relating the ISA adoption. The examination of every psychological construct of the behavior of the employees can help the IS managers to identify (while they measure the ISA adoption level in their organization) the reasons why the individuals choose to adopt a certain behavior. Layton (2005) developed POST™ framework in order to help the IS managers to arrange short measures so as to identify the awareness of the employees relating to the ISP and rules of the organization.

The affection of the psychological construct of motivation to the behavior of the end users that adopt ISA or not can be discovered with the use of the background theory of the need theory (Maslow, 1943);(Layton, 2005), the two-factor theory (Herzberg, 1966); (Layton, 2005), the operant model, the goal-setting theory, the expectancy theory, and the equity theory. The construct of motivation is about the motives of the end users relating the world around them and their internal world. For the need theory these motives are related with the physiological, safety, social, ego and self-actualization needs of the individuals. So the individuals take their final decisions after they have covered all of their needs.

Two factor theory connects the dissatisfaction of the individuals with the bad working environment, and the operant model supports the positive or negative reinforcement of the individuals in order to adopt a certain behavior. For the goal-setting theory it has to be discovered if the operations of the organization and the working environment in general are against the goals that have been set by the individuals (for their personal satisfaction). There’s a great relation between the constructs of ethics and beliefs with the expectancy theory, as the theory supports that
the perceptions of the end users influence the way they behave. Finally, equity theory examines the desires of the individuals to have the same rights with the others or to be treated by their supervisors in the same way like their fellows (Layton, 2005).

The psychological construct of attitude is consisted by three components (Organ and Bateman, 1986); (Layton, 2005, p.80): 1) the affective component, which helps to examine the negative feelings that might be caused to the end users when they hear, read or see something relative with the IS field, 2) the cognitive component, which is about the beliefs of someone for something and helps to discover if the beliefs of the individuals are in contrast with the organizational ISP and 3) the behavioral component which helps to understand if the adopted behavior of the end users is related with their attitude (Layton, 2005).

Supporting theories for the identification of the affection of personality to the behavior of the end users is the motive based approach and the trait based approach. The motive based approach is about the motives of the end users that make them to adopt or not ISA (similar to the construct of motivation). The trait based approach is known as the “Big Five” traits, which traits are: the openness to experience, the conscientiousness, the extroversion / introversion, the agreeableness and the neuroticism (Layton, 2005). Kajzer et al. (2014) make use of the trait based approach and argue that the personality of the individuals influences their compliance with the organizational ISP.

Examining the psychological construct of the beliefs can help to discover the opinion of the individuals for the world around them. The beliefs of the individuals formulate their behavior, so the IS managers can discover if the end users internalize the meaning of ISP while examining what are their beliefs about the IS issues. In addition, the psychological construct of ethics is connected with the construct of the beliefs, as the ethics concern the way that the individuals interact with the world around them. If the individuals support an ethical theory because they believe that it is related with their behavior, then they will adopt ISA or not depending on how similar are the ISP and IS rules of the organization with the ethical norms that they support.

The psychological construct of morals helps IS managers to discover the individuals’ opinions about what is right to be done or not. Layton (2005) stresses that morals and ethics are at the very core of the individuals. In addition for the Author the main reason that the end users don’t understand the negative consequences of not adopting ISA is that they don’t understand the ethical dimensions of the ISP and the IS issues in general. So the Author relates the construct of morals with the construct of ethics and stresses that the one construct is based upon the other.

Layton (2005, p.119-123) presents Kohlberg’s moral development and Gilligan’s moral growth as supporting theories for the construct of morals and states that each of the two theories has three phases: the preconventional, the conventional, and the postconventional. In addition the Author argues that according to Gilligan the ethical thinking is based on two perspectives: 1) the justice perspective (i.e. understand morality primarily in terms of rules and specify rights and order them by relative importance when they conflict), and 2) the care perspective (kindness and beneficence, maintaining personal relationships, and sensitivity to one’s own needs and those of others in particular circumstances). Carol Gilligan (who inspired many feminists with her work) discovered that Kohlberg’s theory was inadequate relating
the moral development of women because he doesn’t take into consideration the care perspective, so despite that Gilligan agrees with the importance of both the two perspectives (i.e. justice and care), she advanced her theory for the moral growth by a care perspective (Layton, 2005).

None of the psychological constructs of the POST™ framework is independent from the other constructs. In contrast every psychological construct is influenced from the other constructs and influences the other constructs. Also the interaction between the psychological constructs has as result the formulation of the individuals’ behaviors (Layton, 2005)

OCB is a supporting theory to POST™ framework in order to understand the individuals’ behaviors in their working environment. According to OCB the motives of the employees affect their behaviors and their final decision to adopt ISA or not. The most common categories of OCB are the helping behavior, the sportsmanship, the organizational loyalty, the organizational compliance, the individual initiative, the civic virtue, and the self development (Podsakoff et al., 2000);( Layton, 2005, p.37). Despite that the POST™ framework and OCB theories help IS managers to identify how the behaviors of the end users affect their awareness to IS issues and ISP, it is presented that the above theories cannot identify which are the external factors that directly affect the end users and formulate their final behavior.

PEST analysis is the analysis of the external political (together with the legal factors), economic, social (together with the ecology factors) and technology factors (Chaffey and Wood, 2005); Ward and Peppard (2002). The IS managers can use the PEST analysis so as to examine, together with the use of POST™ framework and the aspects of OCB, if the influence of the external factors is the only that define the final behavior and the ISA adoption level of the end users. The difference between POST™ framework and PEST analysis lies on the fact that the framework helps IS managers to identify the affection of the external factors to the behaviors of the end users, but the final decision of which behavior should be adopted remains to be made from the end users. In contrast PEST analysis helps to identify the affection of the external factors to the behavior of the individuals, where the individuals won’t have another choice to adopt a different behavior until the external factors stop to exist (e.g. war).

Numerous measurement tactics have been proposed to identify the ISA adoption level in an organization (Parsons et al, 2014; Maqousi, Balikhina and Mackay, 2013; Kajzer et al, 2014; Kruger and Kearney, 2006). The measurement tactic of POST™ framework differs from the other tactics because it combines all the well defined psychological theories about the behavior of the end users and adjusts them to the IS field. So, it helps the IS managers to arrange short measures in order to identify the ISA adoption level of the employees of their organizations, and understand the reasons why they perform such behavior (mostly for the divergent behaviors).

5.3 Reflections

In this study it is tried to be evaluated the affection of the psychology of the employees to their behaviors when they decide to adopt ISA or not. The POST™ framework was chosen as the representative background theory that supported the researcher for developing a measurement tactic in order to discover the ISA adoption
level in the IT company, and then to analyze the collected data in order to identify the reasons that the employees choose to adopt a certain behavior. Also the framework enhanced the ability of the researcher to examine which psychological constructs of the individuals’ behaviors are mostly affected by the internal and the external factors and how can these psychological constructs influence the other constructs.

The background theory of POST™ framework is highly depended on well structured psychological theories that have been adjusted in the IS field of knowledge. The researcher has a previous academic knowledge in the psychology field as he has attended a course in psychology in the third year of his bachelor studies, also he has been working as an IS manager in the Greek military from 2011 to 2014. So the decision of using the POST™ framework was based on the belief that the end users have to internalize the meaning of IS in order to be right to their obligations and to adopt ISA (Siponen 2000; Layton, 2005). Although the previous knowledge of the researcher in the psychology field and the aspects of OCB, it was very interesting experience to discover the way that the psychological constructs of the behavior have been adjusted in the IS field. Also it was important to learn how the IS managers of the organizations can measure the ISA adoption level of the employees so as to increase the ISA adoption level in their organization. If the IS managers want to discover the affection of the employees’ behaviors to their final decision to adopt ISA or not (i.e. if they want to understand the “why”), then they cannot measure the ISA adoption level of the employees in their organizations in a direct way (Layton, 2005). In order to measure the ISA adoption level in an indirect way, then the IS managers have to be based on previous knowledge about the relation between psychology and behavior, and Layton (2005) provides much knowledge in this field with the POST™ framework.

Reading previous knowledge about how the psychology affects the behavior of the individuals in order to adopt ISA or not (please see chapter 2), then it was discovered that Layton (2005) incorporates in the POST™ framework the majority of that knowledge and divides it to six psychological constructs (motivation, attitude, beliefs, personality, morals, and ethics). It was surprising to discover that Layton (2005) didn’t base the framework only on certain well structured psychological theories that are adjusted in the IS field and that he presents in the background theory of every psychological constructs many statements from other Authors that have conducted researchers in the same field of knowledge. The framework cannot be considered as limited because after trying to present the affection of the external and internal factors to every psychological construct, it gives the ability to IS managers to add any additional theory they like (similar with the context of every psychological construct). The researcher decided to use the framework as he noticed that it can help him to completely understand why the employees in general choose to adopt ISA or not.

The use of the PEST analysis was based on the assumption that the external environmental factors can sometimes directly affect the behavior of the individuals. More specifically there were born thoughts about the way that the individuals would behave if they were affected by “extreme” environmental factors (e.g. earthquake). The belief of the researcher is that in this case the individuals become “victims” of the environmental factors and adopt a certain behavior because they are obligated to do it, even if they don’t want to adopt that behavior. The above assumption was supported after the analysis of the data, when it was discovered that the financial situation of
Greece and the external social environment leads the SMEs to the decrease of the employees’ salaries and not to acknowledge the importance of the training programs.

It was preferred the qualitative and more specifically the interpretive type of research, as there was a trial to understand the internal thoughts of the individuals about the IS issues in general and the relation between the “reality” of the individuals and the world around them (Myers, 1997). The conduction of the study in the IT company was a very important experience. The IT company agreed to cooperate with the researcher after he sent an email to the general manager of the company in which he informed him about the purposes of the study, the type of the study and the ways for the conduction of the interviews, see Appendix A. The arrangement of the semi-structured interviews, the conduction of the semi structured interviews, the collection of data and the analysis of data gave the ability to learn in practice the difficulties when trying to measure the ISA adoption level in a company. Also the interviews provided knowledge about how should the IS managers of the organizations develop their measurement tactics so as to identify the ISA adoption level of the employees (in an indirect way).

The development of the measurement tactic that has been used for the conduction of the study in the IT company was very difficult. The researcher had to read the background theory of every psychological construct many times so as to discover which questions would be the most representative (according to what Layton (2005) describes for every psychological construct) in order to examine the level of the influence of every psychological construct by the internal and the external factors. But the questions had also to be “open” questions in order not to provide certain answers and in order to give the stakeholders the ability to free express their opinions. So after making a lot of questions, then the most neutral questions were preferred to be included in the interview guide. All of the questions facilitate on the one hand the researcher to examine the reasons that the employees adopt a certain behavior when they choose to adopt ISA or not, and on the other hand the questions remain “open” questions so as to leave the stakeholders to give their answers without to be lead by the researcher. The neutrality of the developed interview guide was checked also by others (i.e. other students, the IS manager of the IT company and the supervisor), and their feedback altered the way that some questions were used.

It can be stated that there is a possibility that the formulated interview guide can be considered as not neutral, as its aim is to uncover the internal world of the employees regarding their motives, attitude, beliefs, personality, morals and ethics. But the interview guide examines the individuals’ behaviors as employees in an organization and not as people in the society. Thus the stakeholders were free to reveal the amount of the information they wanted about themselves in order to help the researcher to identify the ISA adoption level in their company (Kenneth and Herman, 2008), and the above is depended on the importance that is given by the individuals for the IS in general.

Before the conduction of the interviews it was given to the stakeholders an informed consent form that informed them about the interview procedure, the aim of the study and their rights. Also the stakeholders were informed that the researcher’s intention is to respect their privacy and that they could avoid giving answers to any question they didn’t like or they could stop the interview any time they wanted. During the interviews the stakeholders were free to express their opinion for any
theme and there were additional questions when needed. If the researcher noticed that a stakeholder was hesitant to answer a question then he asked the stakeholder if it was better not to answer the question and move to the next question.

The questions in the interviews, the speaking language in the interviews, the collection of data and the analysis results were in the Greek language. The interview guide and the final results were translated from the Greek language to the English language. After the translation process it was discovered that some translated questions can lose their meaning and seem to lead the stakeholders to provide certain answers, but this is a consequence of the use of tones in the Greek language and none of the questions was a leading question.

Although all of the difficulties for the formulation of the interview guide, the collection, the analysis and the translation of data, it was a very enjoyable procedure to get involved in the IS field and to communicate with other people so as to attain the purposes of the research. The suggested refinement of the POST™ framework was decided to be implemented after the analysis of data and the provision of the final results. The POST™ framework refinement together with the 9 steps for the development of ISMSs present the suggestion of the researcher to the IS managers of the organizations so as to measure the ISA adoption level of the employees and link the measurement results to their ISMSs.
Chapter 6: Concluding remarks

Chapter 6 contains general conclusions about the use of theory, the research process, and the provision of the final results. Also, it is presented an argumentation about the contribution of the thesis to the research area of the IS field and then the chapter ends with the Author’s statements about the needs for future research.

6.1 Conclusion

The aim of this thesis was to identify whether and why the employees of the IT company did or did not adopt ISA, and whether there were similarities between those who adopted and those who did not adopt ISA. Also great focus was given into the exploration of how could the above findings be used for the development of an ISMS that would try to ensure that all of the employees of the IT company would adopt ISA. After that the first objective was the development of a measurement tactic for the collection and the analysis of data, based on the use of the background theory. The second objective was the development of a methodology which can be used by the IS managers so as to link the measurement findings to the development of ISMSs.

It can be stated that the researcher afforded to attain the aim of the study by the review of the background theory relating the affection of the psychology of the employees to their behaviors, and in turn to their ISA adoption level. Also the aim was attained by the conduction of the study in the IT company and the provision of the final results. In order for the first objective to be attained, there was developed a interview guide and there were conducted semi-structured interviews with stakeholders from the IT company. The collected data were analyzed while using a thematic analysis and a PEST analysis. Furthermore the background theory of the POST™ framework helped in the first phase of the analysis to understand the reasons why the employees adopt ISA or not. Then the PEST analysis helped to discover if the above reasons were directly affected by external factors. The final outcomes presented that the external economical and social environment of Greece directly affected the behavior of some employees, thus it is suggested a refinement of the POST™ framework as a theory and as a measurement tactic. After the provision of the final results it was developed a methodology that contains 9 steps and can be used by the IS managers of the organizations so as to link the measurement findings to their ISMSs. So the second objective of the research was attained by the suggestion of the above methodology.

Two research questions were developed and used as a map from the researcher in order to attain the thesis’ goals:

How the ISA adoption level in an organization can be identified?

POST™ framework has been developed so as to help the IS managers to arrange short measures in order to identify the ISA adoption level of the employees (and the reasons they choose to adopt a certain behavior) in their organizations. So, the framework was used for the conduction of a study in an IT company and it was tried to measure the ISA adoption level of its employees. The analysis of the measurement results was based both to the background theory of the framework and to the conduction of a PEST analysis. It was found that despite the fact that all of the
employees of the IT company adopted ISA, they were found to present similar characteristics in their behavior with the behavior of the end users that are presented in the relative literature as those that don’t adopt ISA. The use of POST™ framework helped to understand why the employees of the IT company performed such behaviors, and the use of PEST analysis helped to discover the affection of the external environment.

How can the measurement findings be linked to the development of ISMS by the IS managers of an organization?

The results of the measurement findings were used for the development of an ISMS that takes into consideration the desires of the employees and tries to satisfy their needs. Unfortunately the affection of the external economic and social environment of Greece to the operations of the IT company, makes it difficult for its IS manager to ensure that all of the employees of the company will adopt ISA without to be unsatisfied. But the IS manager will be in the position to know the “weak points” of IS security in the company, and then he will try to limit their consequences to the safety of the company.

Nine (9) steps (preparation, develop /renew the company's ISP – Rules, communication of the ISP, implementing the ISP, arrange ISTPs – training, supervision – control, measurement of ISA adoption level, ISMS development, and ISMS implementation) which can help the IS managers of the organizations to link the measurement findings of the ISA adoption level to the development of ISMSs are suggested. Also a refinement of the POST™ framework relating the ways of the analysis of the collected data, after the measurement of the ISA adoption level in an organization is suggested. The first step of the analysis is to distinguish the employees that adopt ISA, from the employees that don’t adopt ISA, and the employees that adopt ISA but they perform similar characteristics in their behaviors with those that don’t adopt ISA. The next step is the identification of the reasons that make the above last two categories to perform such behaviors, and the step after is to conduct a PEST analysis in order to discover if the behavior of the employees is directly affected by external environmental factors.

6.2 Contribution

This study illustrates the great affection of the behaviors of the employees to their final decision to adopt ISA or not. One of its contributions to the IS field of knowledge is that it presents a methodology for the development of a measurement tactic in order to identify the ISA adoption level of the employees in an organization. Initially suggestions about the the type of the research (i.e. qualitative) were provided followed by an an interview guide for the conduction of semi-structured interviews with the stakeholders. Finally, a methodology for the analysis of the collected data, were analytically presented.

A second contribution is the refinement of the POST™ framework as a theory and as a measurement tactic. As it was shown by the conduction of the study in the IT company, external environmental factors can in some cases directly affect the behavior of the employees. Thus the implementation of the background theory of PEST analysis as an additional theory to the framework (i.e. like OCB) and the use of
PEST analysis as the second “filter” of analysis of the measurement findings were sugested.

The third contribution is the presentation of a methodology that can help the IS managers of the organizations to link the measurement findings of the ISA adoption level of the employees in the organization to the development of ISMSs. The suggested methodology is consisted of 9 steps and can be used for organizations that implementing their ISP for the first time or for organizations that want to increase the ISA adoption level of their employees.

6.3 Future Research

There is a need for the conduction of many studies that will make use of the POST™ framework in order to improve the framework both as a theory and as a measurement tactic. The conduction of additional researches will help to discover the influence of every psychological construct to the behavior of the end users that adopt ISA or not. If the measurement findings represent all of the reasons that make the employees to adopt a divergent behavior, then the IS managers will be in the position to develop ISMSs that will try to increase the ISA adoption level in their organizations. Also there’s a need for the further development of the framework as a measurement tactic, so as to provide several measurement “tools” depending on the type of the organization.

The reliability of the refinement of the POST™ framework has to be checked by researches that will be conducted in a higher amount of population and in more organizations than the current study. Also it has to be discovered the effectiveness of the developed ISMS that will be based on the measurement findings (even if the measures will be made only with the use of the framework) with the conduction of additional measures through the pass of time. In the same direction, there’s a need to identify how effective are the suggested 9 steps for the development and the implementation of ISMSs and the creation of an IS climate in the organizations.
References


**Online Sources**


Appendix A (Email to the IT Company)

Dear General Manager of the Company,

My name is Bladimiros Spandonidis and I study Information Systems at an internet-based Master program named Information Systems/linnaeus University of Sweden. I’m writing to you to ask your cooperation, if it is possible, for the conduction of a research to your company. This research is going to be conducted in order to make my Master Thesis for the above Master Program. More specifically, the Master thesis will concern the linking of information security with the information security management strategy. The guiding theory for the research will be the POST (TM) Framework of Timothy P. Layton Sr.(2005) and it will help the researcher in cooperation with the managers of your company to identify the level that this framework helps for the measurement of the employees’ information security awareness. Also the outcomes of the research will help for the evaluation and the reformulation of the framework.

The above research will be important for your company, as it will develop the basis for the plan of your management strategy. It would be nice if you could offer to me some of your valuable time and your employees’ valuable time for the conduction of interviews based on an interview guide that will be checked by you.
Appendix B (Interview Guide)

Organizational Citizenship Behavior (OCB).

1. Do you think that every employee needs to do only what is described in his/her job requirements or only what his/her supervisor told him/her to do?
2. (ONLY FOR IS MANAGERS) Which is according to your opinion the properly behavior for an employee?
3. Can you easily cooperate with the other employees in the company?
4. Do you like to help other co-workers?
5. What are the things that you don’t like in the culture of the company?
6. Are you satisfied with your job?
7. (ONLY FOR IS MANAGERS) Do the employees complain when they have more job to do?
8. Do you like the participation in the company’s meetings?
9. What are you doing for your self- improvement as an employee of the company?

User Behavior & Motivation

1. Are there any information security training programs in your company?
2. (ONLY FOR IS MANAGERS) How do you ensure that all the employees have understood the meaning of being complaint with information security policies and they have internalized this meaning?
3. (ONLY FOR IS MANAGERS) How do you treat the employees that don’t respect the company’s information security policies?
4. How would a reward or a punishment influence your working attitude, would all of this make you to give more focus to information security issues?

Motivation

1. Are you good at work? What do you believe that makes you work in this way?
2. What do you dream to attain?
3. Are there any facts that make you to be tired and feel disappointment for your work?
4. Do your motives influence the way that you treat the information security policies of your company?

Attitude

1. What are your feelings when you read the information security norms?
2. What are your feelings when you see or listen messages relative with information security?
3. (ONLY FOR IS MANAGERS) What are your criteria for the construction of messages relative with information security?
4. What is your opinion about information security?
5. Do you apply all the information security norms under any circumstances?

Personality

1. Can you make a description of your personality?
2. Do you put goals that you much reach into your life and your work?
3. How strict are you with yourself in order to reach your goals?
4. Would you reveal critical information of the company for personal benefit?
5. Do you like gossip?
6. Would you give the personal code of your computer to a colleague to help him make faster the job?
7. Are you open to new experiences?
8. Are you organized?
9. Are you quick to your decisions?
10. How difficult is for you to change your decision about something?
11. Are you careful towards yourself and others?
12. Do you like working in groups or alone?
13. Can you easily cooperate with others?
14. Do you easily get influenced by others?
15. Do you have a moody character?
16. Do you think your personal problems while working?

Beliefs

1. What is your opinion about the information security norms of your company?
2. Why do you think that it is important to be complaint with the company’s information security policies?
3. What is your opinion about the companies applying strict rules for the security of their information?
4. Which is the right punishment for those that don’t respect the company’s information security policies?
5. What is your opinion for the information security training programs?

Ethics

1. Why should not steal?
2. Is it right the electronic monitoring of the employees at work?
3. Should we all the time be right towards our obligations?
4. Do you think that the implementation of information security rules must not be applied if it does not serve the needs of the group (e.g. delay at work) or should we judge from the case before we act?
5. Do you think that the various antivirus are enough to protect you from hackers?
6. Have you been informed in the past about the world’s ethical rules of computing and using of internet?
7. What should be in your opinion the ethical rules of computer and internet use?

Morals

1. Would you care for a colleague so much so as to serve him/her knowing that your movement will entrust your daily routine with more work?
2. You trust your colleagues so much, that you don’t believe that they will ever reveal any critical information of the company that you are supposed to handle?
3. How would you judge the behavior of an employee who negligently revealed critical information of your company?
4. (ONLY FOR IS MANAGERS) Knowing the dangers that exist in information security, do you believe that it would be unethical not to train properly your company’s employees?
Appendix C (Informed Consent Form)

Date:.........................


Re#: Bladimiros Spandonidis, SOA STAIDKI 3, Alexandroupoli, ZIP Code: 68100. Telephone number: +30 6937022597 - +306940403245, Email: bladimiros.x@gmail.com, bs222ek@student.lnu.se

Purpose of the Research: The purpose of this research is to examine all the criteria that affect the implementation of information security awareness in an organization and after that to link the development of this awareness with the overall information security management strategy. Furthermore, it is going to examine the factors that affect the compliance of the employees with information security policies and attends to create knowledge and identify methods which will ensure that in every case the managers of an organization will be in the position to measure the employees’ security awareness, to develop suitable training programs and information security policies (according to the measurement findings), and to ensure that there won’t be a leakage of the organization’s secured information. The outcomes of the research will illustrate all those areas that need more attention from the scope of the IS managers and all those areas that need further investigation and reformulation from the scope of the researchers (i.e. reformulation or expansion of the POST™ framework). A final purpose of this research is the creation of a knowledge background for the IS managers that will be used as a tool in order to help them to create their own information security strategies according to the “psychology” of their employees.

What You Will Be Asked to Do in the Research: You will be asked to work with the researcher so that we can get you a few minutes interview on issues related to the way you perceive the awareness in information security based on your character, as well you will be asked about your opinion on information security.

Risks and Discomforts: We do not foresee any risks or discomfort from your participation in the research.

Benefits of the Research and Benefits to You: This research is going to identify in practice all those steps that are needed from the IS managers of an organization in order to understand of which are the key points for the adoption of an information security policy in their organization, to define tactics so as to evaluate the level that their organization is secured from a compromise of classified information, to arrange information security training programs and to develop an information security management strategy. Also, it attends to investigate the importance of the development of information security awareness in an organization for both of its IS managers and employees, and it tries to identify all of those methods that can be adopted in order that there will be created a methodology for the “measurement” of the information security awareness in an organization.

Voluntary Participation: Your participation in the study is completely voluntary and
you may choose to stop participating at any time. Your decision not to volunteer will not influence the (treatment you may be receiving, nature of the ongoing relationship you may have with the researchers or study staff) nature of your relationship with Linnaeus University either now, or in the future.

**Withdrawal from the Study:** You can stop participating in the study at any time, for any reason, if you so decide. Your decision to stop participating, or to refuse to answer particular questions, will not affect your relationship with the researcher, Linnaeus University, or any other group associated with this project. In the event you withdraw from the study, all associated data collected will be immediately destroyed wherever possible.

**Confidentiality:** Your identity will not be revealed and your full names will not be exposed during and after the research. All information you supply during the research will be held in confidence and unless you specifically indicate your consent, your name will not appear in any report or publication of the research. The data will be collected by recorded interviews or by simple interviews if you won’t accept to be recorded. Your data will be safely stored in a locked facility and only researcher and his supervisor will have access to this information. The data will be destroyed after the completion of the Master Thesis. Confidentiality will be provided to the fullest extent possible by law.

**Questions About the Research?** If you have questions about the research in general or about your role in the study, please feel free to contact Bladimiros Spandonidis either by telephone at +30 6937022597 - +306940403245 or by e-mail bladimiros.x@gmail.com , bs222ek@student.lnu.se.

**Legal Rights and Signatures:** I consent to participate in “Linking the Information Security Awareness to the Information Security Management Strategy/Master Thesis at Linnaeus University of Sweden” conducted by Bladimiros Spandonidis. I have understood the nature of this project and wish to participate. I am not waiving any of my legal rights by signing this form. My signature below indicates my consent.

Participant………………………………………………

Date……………………………………………………

Signature………………………………………………
## Appendix D (Research Process)

<table>
<thead>
<tr>
<th>Question</th>
<th>Scope of the question</th>
<th>Answer to the question</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What</strong></td>
<td>Intended to research</td>
<td>Explore the adoption level of ISA of the employees in an IT Company and link the outcomes to the development of an ISMS</td>
</tr>
<tr>
<td><strong>Why</strong></td>
<td>The research is needed</td>
<td>There isn’t a research that examines the above while using POST™ framework and PEST analysis</td>
</tr>
<tr>
<td><strong>How</strong></td>
<td>The research was done</td>
<td>Qualitative-interpretive, exploratory research. The collection of data is based on semi-structured interviews with stakeholders</td>
</tr>
<tr>
<td><strong>When</strong></td>
<td>The research was done</td>
<td>It started by March and it finished by June of 2015</td>
</tr>
<tr>
<td><strong>What</strong></td>
<td>Resources needed</td>
<td>Literature for reading, stakeholders for interviews, internet connection, cooperation with supervisor, and a digital recorder</td>
</tr>
<tr>
<td><strong>Who</strong></td>
<td>You talked to</td>
<td>IS managers and employees of the IT Company</td>
</tr>
<tr>
<td><strong>Where</strong></td>
<td>The data was</td>
<td>In the stakeholders (while working or not)</td>
</tr>
<tr>
<td><strong>How</strong></td>
<td>Access the data</td>
<td>Request from the company to conduct the research, approval, distribution of a written form of consent for the stakeholders, arrangement of semi-structured interviews with individuals</td>
</tr>
<tr>
<td><strong>What</strong></td>
<td>The outcomes were</td>
<td>Development of a measurement tactic while using the POST™ framework and PEST analysis, expansion of the theory of the framework, linking ISA to the development of ISMS</td>
</tr>
</tbody>
</table>