5-14-2015

Information Security Policy for E-government in Saudi Arabia: Effectiveness, Vulnerabilities and Threats

Khaled AlGarni

R.I.T

Information Security Policy for E-government in Saudi Arabia:

Effectiveness, Vulnerabilities and Threats

By

Khaled AlGarni

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Networking and System Administration

Department of Information Sciences and Technologies & Computing Security

College of Computing and Information Sciences

Rochester Institute of Technology
Rochester , NY
May 14, 2015

Thesis Committee

Name Date

Tae Oh 05/12 /2015
Chair

Jonathan Maurer 05/14/2015
Committee Member

Young B. Choi. 05/12/2015
Committee Member

Acknowledgment

I would like to express my special appreciation and thanks to my thesis committees, professor. Tom Oh, professor. Jonathan Maurer, and professor. Young B. Choi, for their patience, motivation, enthusiasm, and immense knowledge.

Also, I would like to thanks all participants that participated in the research study for this thesis.

Finally, I will not to forget to thank my parents that give me all support that I need when I was child until now, also, I would like to thank my wife and my son Mishaal that they give me a good atmosphere and encourage me in my studies.

Abstract

This study focuses on the issue of information security policy for e-government in Saudi Arabia. It evaluates the three fundamental pillars that determine data security such as effectiveness, vulnerabilities, and threats. The paper is seeking to reveal the risks of information security policy for e-government in Saudi Arabia as well as to examine the vulnerabilities and the effectiveness of the system.

The methodology applied inductive approach where both qualitative and quantitative research method were used. A survey by use of questionnaires and an interview was conducted.

Execusive Summary

Introduction: In many countries, the implementation of e-Government has proved useful in providing efficient services to consumers. Such a program increases work speed and causes no unnecessary delays. This study assesses the effectiveness of Yesser, the e- government program that Saudi Arabia adopted in 2007. This study also provides recommendations to improve the security of the Yesser Program, to further professionalize IT specialists, and to increase the level of consumer participation, which will improve of the quality of life for Saudi citizens.

Literature Review: The primary purpose of producing literature review is to support the findings of this study via the theoretical justifications obtained from literature. The review revealed that in Saudi Arabia, there is the absence of agencies to monitor the accountability of e-government services. Most of the workers of offices in Saudi Arabia lack professionalism, and this is a great weakness in the implementation of appropriate policy for e-government. In order for the government to solve this problem, it needs to restructure these rules and regulations to attain online transactions that are more democratic and transparent. In order to have an effective and efficient implementation of the e-government program, there must be qualified personnel to perform such a task. The absence of such staff in Saudi Arabia poses a major challenge to the IT policy. The government of Saudi Arabia should come up with highly training programs in addition to sufficient number of IT specialists.

Research Methodology: The research method for this study uses inductive approach and a mixed design following the philosophy of positivism of case study. Data for the case of Saudi Arabia is collected via primary source and the instruments are questionnaire survey (quantitative part) and face-to-face interview (qualitative part). Quantitative data analysis includes frequency distribution, clustered bar graphs, and pie charts. Analysis of qualitative data is a three-step process that includes reducing the data, displaying the data, and verifying or drawing conclusion.

Findings: The current study has identified those organizational and technological issues that affect the information security in Saudi Arabia at national level. Moreover, many areas are highlighted where modifications can make the practice of e-government safer. The measures taken by Saudi government in developing organizations are far admired than the cultural development. Lack of awareness in the citizens and inadequate training of the employees dealing with e-services is not satisfactory. Moreover, the most advancing measures taken to reduce security threats of information shared via internet are infrastructure development. However, it needs to be updated regularly as the challenges to information security are always changing. Despite all the attempts to ensure information security in e-government of Saudi Arabia, trust of the citizens in the applications is still low. Thus, Saudi government must given priority to the awareness programs.

Table of Contents

List of Tables

List of Figures

CHAPTER 01: INTRODUCTION

1.1 Introduction

The topic is related with the implementation of an Information Security Policy to facilitate the functions of e-government in Saudi Arabia. The three major factors that need to be assessed in detail are the effectiveness, vulnerabilities, and threats of an Information Security Policy. It is a fact that the importance of Information Security is very high for any Government Agency. The basic purpose of the Information Security is to ensure the protection of data resources and uphold three pillars of data security. The three pillars include confidentiality, integrity and the availability of data. The adoption of an effective security mechanism also becomes necessary for the adequate protection of data. The usage of the e-government requires the usage of Information Technology to deliver its services to the citizens. The protection of e-government services is essential in order to increase the confidence of the people in using these services. In many countries, the implementation of e-government has proved useful in providing efficient services to consumers. Such a program increases work speed and causes no unnecessary delays. This study assesses the effectiveness of Yesser, the e- government program that Saudi Arabia adopted in 2007. This study also provides recommendations to improve the security of the Yesser Program, to further professionalize IT specialists, and to increase the level of consumer participation, which will improve of the quality of life for Saudi citizens.

1.2 Background

Information security is of major importance to every government agency. The role of information security is to ensure protection of data resources and uphold the three pillars of data security. These pillars comprise confidentiality, integrity, and the availability of data. In order to offer appropriately adequate protection of data, a security policy which security mechanisms are devised. e-government involves the use of information technologies to deliver its services to the citizens. There are many benefits to improved information security:

First, better services to consumers by making them feel more confidence about e-government program.

Second, Information security contributes to the general economic development of the country as creates the foundation for sustainability and effective interaction of different branches of the economy. Governments typically provide the realization of principles of information security as they have the necessary amount of resources. The Information Security Policy may be successfully realized in Saudi Arabia. It will allow reaching a number of objectives. First, the structure of internal businesses may be optimized, as the information flows will become more efficient. It will also be beneficial for international relations of the country. If information security is achieved, additional investments from abroad may be received. Thus, Saudi Arabia may strengthen its competitive positions in the international investment market.

Third, the Information Security Policy for e-government may increase the effectiveness of the country's government in solving key economic and social problems. As government officials have additional sources of relevant and objective information, they will be able to adjust their policies accordingly. In general, the Information Security Policy may be beneficial for Saudi Arabia in the long run as the country's competitive positions may be strengthened. The country may be able to become not only the regional leader, but the global one, as well.

1.3 Problem Statement

Privacy of information provided through the Internet has been a major concern in Saudi Arabia. Citizens are reluctant to give their information through the Internet, as they fear their private information might get into the hands of unauthorized individuals. Such information, and especially information about financial transactions, may be used in hacking of citizens' accounts. The security policy is not comprehensive enough to guarantee the security of e-government services in Saudi Arabia. The study is going to reveal the threats of information security policy for e-government in Saudi Arabia as well as examine the vulnerabilities and the effectiveness of the policy.

1.4 Significance of the Study

The research study is worth for a number of reasons. Firstly, it will help in assessing the degree of effectiveness of the present security policy, security holes in the policy, and threats not addressed by the policy. It, in turn, would help in coming up with measures of ensuring that the policy is security-oriented, which increases citizens' confidence in using e-government services.

1.5 Research Question

In order to achieve the objectives of the study, the following research questions will ensure that the study remains focused on the main issues:

1. What are the security mechanisms defined in the security policy for the protection of e-government services?
2. What is the degree of effectiveness of the security mechanism defined by the security policy in protecting e-government services?

1.6 Aims and Objectives of the Study

The objectives that the study will seek to accomplish will include:

1. To determine the degree of effectiveness of the current security policy in securing government services provided electronically;
2. To determine security holes in the present security policy;
3. To determine the threats that security holes not addressed in the policy are likely to pose to the e-government services.

1.7 Research Contents

This research consists of five chapters. The first chapter is an introduction to the work. It has provided with the background of the study and identified a research problem. Moreover, the research questions to be answered and the aims and objectives of the study are given in this chapter. The second chapter presents an extensive review of literature. It presents an overview of the previous studies done on the similar subject. The third chapter is research methodology which describes the details of the whole procedure of the study. It is written in a manner that other researcher can refute this research. The fourth chapter presents all the results of this study obtained following the procedure as described in the third chapter. The last fifth chapter concludes the study presenting an overview of the research and suggesting implications and recommendations.

1.8 Summary of the Chapter

In many countries, the implementation of the E-Government has proved to be useful in providing efficient services to the consumers. This increases the speed of the work and does not cause any unnecessary delays. All these aspects matters for the efficient service of the Government work. In the end, it proves to be beneficial for both Government and the citizens living in Saudi Arabia. Therefore, in this study, all the issues related to the Information Security Policy will be discussed in detail. The research study is worth for a number of reasons. Firstly, it will help in assessing the degree of effectiveness of the present security policy, security holes in the policy, and threats not addressed by the policy. It, in turn, would help in coming up with measures of ensuring that the policy is security-oriented, which increases citizens' confidence in using e-government services.

CHAPTER 02: LITERATURE REVIEW

2.1 Introduction

Knowledge expanded based on the previous research is refutable and consistent. Therefore, the very first step towards the solution research problem is to overview the findings of previous research. For this purpose, this chapter reviews the publications and literature. Different themes are identified from the previous studies and are summarized here. Moreover, the primary purpose of producing this chapter is to support the findings of this study via the theoretical justifications obtained from literature.

2.2 Background of the E-Government Services

The development of an Electronic Government System is a technical and political sophisticated activity. The creation of the appropriate policies for the protection of online transactions becomes a major challenge for the Government. The quality of such system has dependence on several factors. The key benefits of e-government for the country may be summarized as follows [10].

1) The benefits for government agencies. The large amount of communications may be optimized. The Information Security Policy for e-government should allow reducing the costs of operations. It is estimated that more than 60% of government online programs lead to cost reductions [10]. The communication costs may be significantly reduced with the help of new technology tools (including emails, the Internet, etc.) that may reduce the “tax burden” for ordinary citizens.

2) The economic benefits for individuals. The citizens of the country will receive additional opportunities for effective control of the government operations. Quality of services is supposed to be optimized and standardized. It means that individuals will be able to adjust their

actions accordingly and form expectations that are more rational. It will increase both the consumer satisfaction and the effectiveness of business operations. The time aspect will be improved, as well. As government and bureaucratic procedures are often time-consuming, the new system will allow minimizing average time spent per operation.

3) The benefits for international trade. The key benefits may be expected in the sphere of international trade. The Information Security Policy for e-government corresponds well to the country's obligations as a WTO member. The electronic infrastructure of the highest quality may allow increasing international attractiveness of business operations in Saudi Arabia. In general, the scales of international trade may be significantly expanded.

4) Contributing to democratic reforms. The open information system is a necessary aspect of any significant democratic reforms in the country. The public will receive information that is more open. At the same time, the significant parts of information will be well protected by government agencies and the new system. Both the public control and information security may be achieved after the implementation of the program. Adequate democratic reforms may contribute to the better competitive positions of the country in the international political arena.

It should be stressed that the purpose of e-government is not only to increase the level of computerization of government structures. It refers to the transformation of the essence of government operations. The structure of relations with citizens and business units are expected to change. Thus, the program will fulfill the valuable social function. In this way, the method of delivering public services will be significantly transformed. It is expected that relationships of partnership between citizens and the government may prevail [11]. Moreover, the scope for corruption is expected to be reduced, as new forms of control will emerge. As corruption constitutes significant obstacles for sustainable development, e-government may minimize this problem.

If the public sphere operates more efficiently, the private sector may receive additional stimulus for its development. As the businesses' costs decline, their expected profits will tend to rise. Thus, the general business activities in the country will become more profitable for companies and individual entrepreneurs. The new system will also encourage the decentralization of administrative functions. In this way, the significance of market forces will increase, and the significance of political factors will diminish.

As the new system allows collecting data for large periods, the processes of learning and improvement may be facilitated. The national government may use available statistics for analyzing its performance and develop ways of its optimization. It will contribute to higher flexibility in government apparatus and bureaucratic system. Additional impulses for the overall development of the country may be created. Higher productivity in one sector may lead to higher effectiveness in other spheres, as well [11]. In this respect, the introduction of the new system may create completely new system of business operations in Saudi Arabia.

However, the functioning of e-government may be organized in a number of ways. In particular, some scientists present it as a four-stage model [12]. These stages include the following.

1. Cataloguing. It refers to possibilities of online presentations and downloadable functions. Thus, it will increase the utility for customers and users.

2. Transaction. It refers to providing relevant links to corresponding interfaces. In this way, the quantity of available functions will be increased.

3. Vertical integration. It refers to the complex integration of different spheres of government.

4. Horizontal integration. It refers to the complex integration of different functions of government.

It may be expected that the new system will allow decreasing the scope of government interventions. In this way, the fraction of the private sector may be increased. Consequently, the productivity within a national economy may be increased, as well. However, it seems that a broader model may be implemented in Saudi Arabia. It may include five stages [11].

1. Online presence. Key government institutions may be constantly present in the internet environment. It will be beneficial for both citizens and government officials. The operating costs will be minimized, and the social issues may be adequately addressed. Moreover, no special technical resources are needed at this stage of the strategy implementation.

2. Basic capability. It refers to the developing of complex central plan. It will address security and other relevant issues. Citizens will be able to submit their information to government institutions through the developed system. It will facilitate the process of analysis and solving main problems.

3. Service availability. New government services will be available in any convenient time for customers. It is reasonable that all services be integrated in the united system of e-government. As the majority of questions are complex and require the joint efforts of different government agencies, the integrate system seems to be the most effective solution. The interests of ordinary users and citizens should be the main concern in this regard.

4. Mature delivery. The system of responsibility should be introduced. Government agencies should become no less responsible than private companies should, as it is necessary for effective implementation of the national reforms.

5. Service transformation. The key purpose of the strategy is a significant improvement of quality of customer services. In order to achieve it, the deep analysis of customer needs should be provided. The e-government should work on the permanent increase of the volume of its operations.

It seems that the development of new technologies and e-government may contribute to the development of digital democracy in the country. In fact, all civilization values may be achieved with the help of the innovative system. However, cultural influence is very significant in Saudi Arabia [13]. Cultural influence is complex and includes both positive and negative aspects. On the one hand, the internet technologies are generally positively appraised by the population. New technologies are recognized as a more effective tool of communication. The values of citizens are perfectly compatible with new technologies, and no strong obstacles were determined in this regard [13].

On the other hand, there is some lack of trust in relation to all government agencies. In this respect, public is not open to the new strategy. Moreover, people consider that government officials are mainly motivated by gaining additional prestige and power rather than solving existing social and economic problems. These factors demonstrate some threats to positive acceptance of the new strategy [13]. Thus, basic human values demonstrate that the general acceptance may be reached only if a higher level of trust in government will be achieved. Therefore, some additional public relations measures may be reasonable, and the total degree of government presence in the economy should be reduced.

Thus, the government has put in place a number of methods in order to protect relevant information. “YESSER” which refers to the Arabic name for the e-government program is faced with a number of challenges in its information security due to a number of reasons [4; 9]. These challenges include the following.

2.2.1 The problem of accountability

In Saudi Arabia, there is the absence of agencies to monitor the accountability of e-government services. Most of the workers of offices in Saudi Arabia lack professionalism, and this is a great weakness in the implementation of appropriate policy for e-government. It is the reason that has made King Abdullah bin Abdul-Aziz to give instructions on the establishment of a board to control the accountability of e-government services [5].

2.2.2 Rules and regulations

One of the challenges of the policy of information security is the complexity of governing these policies, which are centralized. In order for the government to solve this problem, it needs to restructure these rules and regulations to attain online transactions that are more democratic and transparent [6].

2.2.3 Qualified staff

In order to have an effective and efficient implementation of the e-government program, there must be qualified personnel to perform such a task. The absence of such staff in Saudi Arabia poses a major challenge to the IT policy. The government of Saudi Arabia should come up with highly training programs in addition to sufficient number of IT specialists [7].

2.2.4 Internet usage

One of the key difficulties that the implementation of electronic government in Saudi Arabia faces is the usage of the Internet that is considered average. At present, the population of Saudi Arabia that makes use of the Internet is estimated to be about 50 to 55 percent.

The Kingdom of Saudi Arabia has put a number of measures in place in enhancing security when conducting transactions by use of online means. All these measures have been incorporated in the security policy governing ICT infrastructure in Saudi Arabia. Firstly, the government of Saudi Arabia has come up with a center which sole purpose is to ensure the information security awareness besides responding to security incidences. This center, which is referred to as the computer Emergency Response Team (CERT), has been mandated to play both proactive and reactive roles in ensuring awareness and guaranteeing that the ICT infrastructure in Saudi Arabia is secure for both governmental and private organizations. CERT is characterized by its analysis capabilities and its powerful ties that it maintains with the citizens. CERT has been improved to incorporate the coordination of both national and international security incidence response for ICT related incidences. CERT, as stipulated in the information security policy, is part of the communications Information Technology commission (CICT). The objective of CERT includes improving and nurturing awareness, detection, knowledge, prevention, and responding to various incidences of information security [8]. The missions of CERT with regard to information security include the following [1]:

1. To improve on the level of awareness of information security to the people of Saudi Arabia;
2. To be in control of the national effort that is aimed to promote the very best practices of IT security besides improving on the trust of the citizens;

3. To assist in the management of attacks against information security and various other information security related incidences in the Kingdom of Saudi Arabia;
4. To offer to the citizens of Saudi Arabia a trusted environment for electronic transactions;
5. To nurture trust and collaboration between the citizens of Saudi Arabia when carrying out online transactions;
6. To form the point of reference for all information security matters for the citizens in the Kingdom of Saudi Arabia;
7. To develop human capacity and talent in the area of information security to the people in the Kingdom of Saudi Arabia.

More additional measures have been put in place in order to counter security threats in the use of ICT services. An example is Online Transaction Security- Security Operations Center (SOC) [3].

2.3 Role of the Saudi Government

The role of the Saudi Government is very important in exerting maximum efforts for the successful implementation of the Information Security Policy in the Departments. This is going to make their work easy and provide efficient and speedy service to the citizens. The staff will not suffer from work overload and they will learn the IT applications. This will help in improving the competency levels of the employees. Therefore, the Government needs to exert maximum efforts in this regard. The Kingdom of Saudi Arabia has put a number of measures in place in enhancing security when conducting transactions by use of online means. All these measures have been incorporated in the security policy governing ICT infrastructure in Saudi Arabia. An example is the establishment of Online Transaction Security- Security Operations

Center (SOC). The role of this center is to give support to the objectives of CERT in the field of timely detection, timely warning and prevention of information security incidences. This sector will achieve this by monitoring data traffic logs gathered from different devices connected to the national network. Then, the center correlates the patterns for timely detection of anomalies that can serve as a threat to the national network infrastructure. Immediate threats are detected, and security operations center (SOC) delivers this information to Computer Emergency Response Team (CERT) for it to perform the appropriate procedures that can range from having the constituents alerted up to offering them support for the prevention process [2].

2.4 Summary of the Chapter

The primary purpose of producing literature review is to support the findings of this study via the theoretical justifications obtained from literature. The review revealed that in Saudi Arabia, there is the absence of agencies to monitor the accountability of e-government services. Most of the workers of offices in Saudi Arabia lack professionalism, and this is a great weakness in the implementation of appropriate policy for e-government. In order for the government to solve this problem, it needs to restructure these rules and regulations to attain online transactions that are more democratic and transparent. In order to have an effective and efficient implementation of the e-government program, there must be qualified personnel to perform such a task. The absence of such staff in Saudi Arabia poses a major challenge to the IT policy. The government of Saudi Arabia should come up with highly training programs in addition to sufficient number of IT specialists.

CHAPTER 03: RESEARCH METHODOLOGY

3.1 Introduction

Researches Methodology can be described as a way to resolve the research study problem. Research Methodology includes several steps, which are usually taken on by an investigator while carrying out the research [15]. Thus, it might also be regarded as a science of analyzing the way how investigation is carried out systematically [16]. Further, research could be purely based on quantitative data or qualitative data or may be even mix of both. The most important task lies in selecting the correct research paradigm, data collection technique and research approaches. In this chapter, the rationale for using a qualitative research model and characteristics of qualitative research are addressed. Specific topics discussed include case study methodology, data collection and analysis, the role of the researcher, standards of quality and verification, as well as the practices for the protection of the confidentiality of the participants.

3.2 Research Approach

There two broad categories of research in terms of approach employed to reach conclusion: inductive and deductive. Inductive approach of research directs the process form specific observations to a general knowledge while deductive approach of research directs the process from general observations to specific knowledge. The approach chosen in this research is inductive. Hence, specific information at specific time is processed to reach the general conclusion. Inductive approach is more scientific in nature than deductive approach as the conclusion in inductive approach is drawn based on observations rather than theories. Inductive approach is also known as a bottom-up approach, which is a process of using particular instances to infer a general law. The process is a three-step method, (1) systematic observation of the under-investigation phenomenon, (2) identification of themes or pattern in the observation, and

(3) development of the theory with the help of the pattern observed. Following is a schematic representation of inductive approach.

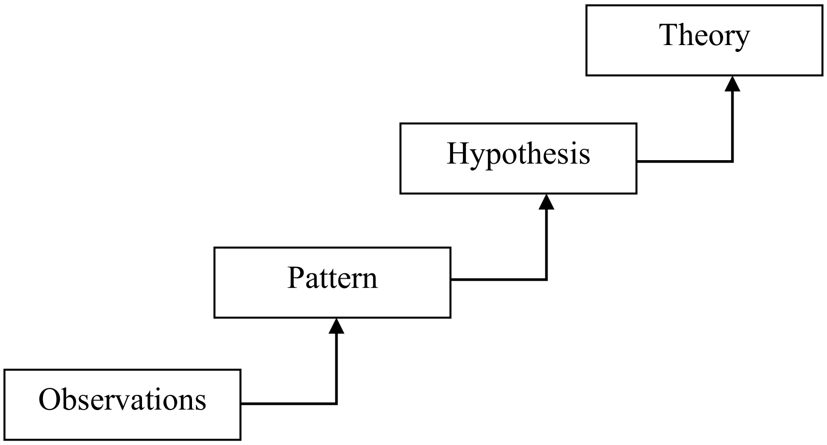

Figure 3. 1: Bottom-up Approach of Research

Observations are the in form of review of the literature and collection of data. Pattern in the collected data is observable via different statistical methods. Another range of statistical method could test the hypothesis, whose results lead to the conclusion of the research, which is a new theory or extension of an existing theory.

3.3 Philosophy behind the Research Approach

The research philosophy is the confirmation about the data that obtained through a specific procedure and later it is analyzed. The current research study covered case study approach as took the case of Libya and secondary sources thus, it is considered as Positivism. In positivism research philosophy, subjective information is derived from analysis of logical and mathematical models. Thus, research is performed under the perspectives of sources of knowledge available for the study. The findings and views that obtain through positivism approach are based on scientific postulates and derive from empirical findings that are holding the views for the society according to the laws, which are particular for each case. This sort of research approach is useful in order to obtain the full understanding within the natural environment and the researchers could not avoid the factors, which may affect the phenomena of the research study. Since, case study and secondary sources have several forms but the researcher has the reasonability to maintain the exact meaning of the scientific knowledge. Thus, positivism philosophy has a glorious approach and it includes a variety of details [17].

3.4 Research Method

In general, there are two kinds of methodology used in explaining hypotheses and analyzing data, Quantitative and Qualitative. This section is an in-depth comparison of quantitative and qualitative methods and there features as found in the literature. After a brief comparison, the chosen method will be stated.

3.4.1 Qualitative Methodology

The qualitative approach is based upon developing a hypothesis, for example, based upon the actual scenario in the construction industry. At the next stage, this hypothesis is judged against the literary evidence of the facts and by interviewing experts. The qualitative approach relies primarily on the collection of qualitative data in form of words, pictures, and objects. This method is employed in many different academic disciplines traditional in social sciences. The qualitative approach introduces information only on particular hypotheses and Quantitative methods can be used to verify which of such hypotheses are true [22]. Additionally, it aims to gathering in-depth understanding of human behavior involves the extensive study of the claims made by the researcher according to the previously conducted work.

3.4.2 Quantitative Methodology

Quantitative approach depends upon the collection of quantitative data such as statistics and percentages. This approach uses a number of methods and models such as time-series analysis and input-output analysis, and often it contains descriptive statistics and inferential statistics in order to test the raw data and to unveil the facts accordingly. In other words, it is the process of presenting and interpreting numerical data. The objective of quantitative research is to employ mathematical models, theories, or hypotheses pertaining to phenomena. Quantitative method is widely used in social sciences such as economics, marketing, and political science [23].

Table 3.1 presents a comparison between quantitative and qualitative approaches for obvious the main differences between them.

3.4.3 Difference between Qualitative and Quantitative Methods

Table 3. 1: Comparison between quantitative and qualitative methods

	Quantitative	**Qualitative**
General Framework	Seek to confirm hypotheses about phenomena. Instruments use more rigid style of eliciting and categorizing responses to questions. Use highly structured methods such as questionnaires, surveys and structured observation.	Seek to explore phenomena. Instruments use more flexible, iterative style of eliciting and categorizing responses to questions. Use semi-structured methods such as in-depth interviews, focus groups, and participant observation.
Data Formats	Numerical	Textual
Analytical Objectives	To quantify variation To predict causal relationships To describe characteristics of a	To describe variation To describe and explain relationships To describe individual experiences

	population	To describe group norms
Question Formats	Closed	Open-ended
Flexibility in Study Design	Study design is stable from beginning to end. Participant responses do not influence or determine how and which questions researchers ask next. Study design is subject to statistical assumptions and conditions.	Some aspects of the study are flexible. Participant responses affect how and which questions researchers ask next. Study design is iterative, that is data collection and research questions are adjusted according to what is learned

Source: [24]

In light of the above analysis, this research employs the quantitative method of study. As the aim of this study is to propose a guideline for development of the construction industry in Libya, this requires generalizing the findings. It is observed that results obtained via quantitative method are easier to generalize than that obtained via qualitative method.

3.5 Case Study Methodology

The case study methodology is appropriate when the purpose of research is to add to the already-existing knowledge about individual, group, or social phenomena and increase understanding of their complexity. The rationale for using a case study strategy is that the researcher explores in depth a program, event, activity, process, or one or more individuals [18]. What made the case study methodology appropriate for this research are three conditions: the type of research questions; the degree of control the researcher has over events being researched; and the focus on the present, here and now, rather than on past historical events. According to Lewis and Thornhill [16], "Interview is considered as one amongst the most rewarding and challenging forms of assessment." In addition, Punch [18] unveils, "interviews call for an individual and adaptability together with the capability to continue within the limits of the planned procedure. During an interview, the person conducting the interview operates directly with the applicant [20] for purposes of this research in-depth interview will enable the interviewer to hold the prospects to explore or put forward questions. For this research further secondary data will be collected from the library, journals, text books, as well newspapers to draw very important conclusions and ideas about innovation. The case study methodology is aptly suited for this research because it is particularistic, descriptive, and heuristic [21], key characteristics for case study research. Particularly, because case studies focus on a particular event, program, phenomenon, or group.

3.5.1 Content analysis

Content analysis is a research technique for making replicable and valid inferences from texts (or other meaningful matter) to the contexts of their use [27]; also, it enables researchers to study human behavior in an indirect way, through an analysis of their communications [28]. Quantitative research uses statistical analysis to demonstrate such concepts as significance, correlation, and relationship between two variables. On the other hand, qualitative research is better suited for determining themes that emerge from data through techniques such as interviews and observations. Qualitative as opposed to quantitative content analysis allows interpretations to be reached that may redefine the original research question. This study used secondary sources for identifying the ways in which innovation ensures competitive advantage. The analysis of text to determine any feelings expressed and any themes associated with those feelings makes qualitative content analysis methodology particularly appropriate to use for this research study. Content analysis can be both a qualitative and quantitative methodology. Strauss

& Corbin [29] summarized the most significant differences between quantitative and qualitative content analysis, indicating that qualitative content analysis is inductive rather than deductive, and that a hypothesis is replaced with an open research question that determines what data is gathered. The studies by [30] described qualitative content analysis, as an iterative process in which trends and patterns may emerge that will alter the nature of the research question that originally defined the study. Krippendorff described it as a hermeneutic circle: The process of re-contextualizing, reinterpreting, and redefining the research question continues until some kind of satisfactory interpretation is reached [31].

3.5.2 Observational analysis

Observations are a good way of gathering information about people's behavior in a natural environment. There are two types of observations structured and unstructured observations. In structured observations, it is predetermined what behaviors are going to be studied. An unstructured observation is more of an investigation to be able to get as much knowledge as possible [32].

3.6 Data Sources

As the approach of the current research is inductive, observations are used to draw patterns. Thus, data collection is the initial step towards the quantitative reasoning. Source of data can be primary or secondary depending on the research question and the availability of the data. Using each of the source type has its own benefits and pitfalls. Although data collection from secondary source saves time and cost, the data is limited and includes chances of biasness. Sometimes, the data available at the secondary source do not provide all the information that is required to answer the research question of the study. On the other hand, primary data eliminated the chances of information loss and increases the credibility of information gathered despite it is time consuming and not cost effective. In light of this comparison between the two sources, data source selected for this research is primary. During the research, data collected from various Government Agencies and Sectors who have knowledge of the ICT system implemented in the Kingdom of Saud Arabia. The respondents are the biggest data source for this project.

3.7 Data Collection Procedure and Sample Size

The collection of the data carried out in the five major cities of Saudi Arabia that includes Jeddah, Riyadh, Dammam, Makkah and Madinah by online. Since the cities are an important hub for the Government services, the adoption of the Information Security policy will prove to be useful for these cities. As part of the study, a thirteen questions survey has been published for three weeks on the Internet at the URL address in [14]. The questionnaire is available on-line in the URL for specialists on Information Technology and citizen in the five cities that are mentioned throughout the social network sites and e-mails to get their opinions without any personal contact. By this way we avoided what happen in traditional survey where direct contact and surrounded might influence personal opinion and mislead the surveyor and surveyed as well. Moreover, the on-line questionnaire increases the number and type of participators. We have reached about three hundred online participators. The sample size was 500 respondents. Every city had to have 100 respondents for the research. The respondents selected for the research given questionnaires by online via URL address in [14].

3.8 Data Analysis

After the collection of data through questionnaire survey, data analysis will be done using frequency distribution, clustered bar graphs, and pie charts. Data collected from interviews can be analyzed in various ways but the choice is to make based on the purpose of the study. According to Locke [25], in unfolding actions, the complexity can be better captured through using the grounded theory. Thus, goal of this analytical technique is building a grounded theory into the data [26]. Miles and Huberman [21] described the most suitable analysis for a research employing qualitative design and collecting primary data through in-depth interview. This analysis is done in a three-step process that includes reducing the data, displaying the data, and verifying or drawing conclusion. Thus, the data analysis in this research is done in the following three steps.

3.8.1 Data Reduction

The gathered responses of the participants can be reduced as follows:

1. Underlining key terms in the responses
2. Repeating the key phrases
3. Reducing the phrases that are similar

3.8.2 Data Display

The reduced data can be either organized or transformed in to graphical representations for display. In this research, the reduced data is organized.

3.8.3 Conclusion and Verification

The displayed data can be used to draw conclusion and verification as follows:

1. Identifying themes or patterns from the displayed data
2. Drawing conclusion in forms of theory from the patterns
3. Verifying these drawing on the basis of existing theory

3.9 Limitations

There are limitations to content analysis research. Qualitative research studies lack general outcomes to the larger population. Instead, the intent is to develop a richer understanding of a particular research topic. Moreover, qualitative studies allow the researcher to explore topics where little research exists. For one thing, it is limited to the examination of recorded communications [28]. The researcher can only analyze the articles that exist. Moreover, the researcher analyzes the articles based on the researcher's lens. The text is subject to the researcher's interpretations Therefore, coding, and journaling help to combat researcher bias and standardize the analytic process. Although there are limitations to qualitative research, there is some measure of validity. Themes emerged from the pattern-coding matrices based on a systematic and transparent coding process. Researcher can be restricted to incorporate those results that are attained by secondary sources.

3.10 Summary of the Chapter

The research method for this study uses inductive approach and a mixed design following the philosophy of positivism of case study. Data for the case of Saudi Arabia is collected via primary source and the instruments are questionnaire survey (quantitative part) and face-to-face interview (qualitative part). Quantitative data analysis includes frequency distribution, clustered bar graphs, and pie charts. Analysis of qualitative data is a three-step process that includes reducing the data, displaying the data, and verifying or drawing conclusion.

CHAPTER 04: RESULTS

4.1 Introduction

This chapter presents the results section of this research. The results are obtained via the questionnaire survey and the semi-structured interview. Thus, there are two sections of this chapter. The first section deals with the responses of the study participants received in the survey. The second section deals with the opinions and views of the study participants received in the interview session. The last section of this chapter summarizes the results.

4.2 Survey Results

Among the active users of internet in any part of the world, young people dominate as they are more up-to-date than the elders. Thus, opinions of young participants might provide a clearer picture of the current scenario of information security of e-government in Saudi Arabia. Fortunately, the sample of the current research is dominated by the young participants. Following is the frequency distribution of the participants' responses for their ages. It can be seen that most of the participants (89.09%) belong to the age group of less than 35 years. However, percentage of elder participants (age group between 35 and 45 years) is also considerable (10.91%). The study involved 25.45% individuals of ages less than 25 years, 63.64% individuals of ages between 25 and 35 years and the remaining were of ages more than 35 years. The sample is a good representative of all age groups.

Table 4. 1: Frequency Distribution of Age

Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Under 25	127	25.45	25.45	25.45
	25-35	318	63.64	63.64	89.09
	35-45	55	10.91	10.91	100
	45-55	0	0	0	100

	Over 55	0	0	0	100
	Total	500	100	100	

As said above, opinions of young participants might provide a clearer picture of the current scenario of information security of e-government in Saudi Arabia due to their chances of bring up-to-date information. Similarly, the participants who frequently use e-government facilities are more likely to come across the pitfalls and limitations in the services especially, in terms of security threat to the information. Thus, the participants in the current study were asked for their frequency of using e-services. Their responses are summarized in the following frequency distribution.

Table 4. 2: Frequency Distribution for the Frequency of Using E Services

Frequency of Using E Service

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Every day	291	58.18	58.18	58.18
	Every week	118	23.64	23.64	81.82
	Every month	73	14.55	14.55	96.37
	Several times a year	18	3.64	3.64	100
	Never	0	0	0	100
	Total	500	100	100	

Majority of the respondent (58.18%) said that they use e-services every day. There was no participant who never used any e-service. Thus, the sample of the current study represents the frequent users of e-services provided by the e-government of Saudi Arabia. Moreover, 23.64%, 14.55%, and 3.64% of the sample belonged to each group of the participants who use e-service weekly, monthly, and several times in a year respectively. After gathering the personal information of the respondents about their ages and their frequency of using e-service, they were asked to provide their responses for different characteristics of the security conditions and other factors of the e-government in Saudi Arabia. They were given choices to respond as ‘agree’, ‘disagree’, and ‘don’t know’. The questions were open ended as every question contained a blank space to write other possible options considered important by the participants. The first question was about the concerns of participants faced while using e-services. Following table illustrates the frequency distributions of their opinions.

Table 4. 3: Frequency Distribution of Concerns in Using E Govt. Services

Concerns in Using E Govt. Services

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	282	56.36	56.36	56.36
	Disagree	127	25.45	25.45	81.81
	I don't know	82	16.36	16.36	98.17
	Other	9	1.82	1.82	100
	Total	500	100	100	

In answer to the question, do you have concerns when you use e-government service? Most of the participants, 56.35%, agreed while a fewer than that, 25.45%, disagreed. Approximately 16% of the respondent said ‘I don’t know’ while approximately two percent wrote other responses including ‘sometimes’ and ‘a few’. Thus, the responses show the provision of e-services in Saudi Arabia by e-government is not flawless and the users face concerns while availing the facility. To observe further the concerns and their types, the respondents were asked to show their agreement or disagreement with other performance indicators of information security in e-government. The responses are summarized as follows:

Table 4. 4: Frequency Distribution for Usefulness and Effectiveness of E-Government

Usefulness and Effectiveness of E-Govt.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	455	90.91	90.91	90.91
	Disagree	36	7.27	7.27	98.18
	I don't know	9	1.82	1.82	100
	Other	0	0	0	100
	Total	500	100	100	

Most of the participating specialists and citizens (90.91%), agreed in response of the question do you think electronic government will be useful and effective to serve the interests of citizens? On the other hand, only 7.27% of the respondents denied the usefulness and effectiveness. Percentage of participants responding ‘I don’t now’ is 1.82%. Thus, citizens and the IT specialists in Saudi Arabia consider the adoption e-government important for the benefit of citizens. Once, the importance of e-government is realized, the attention diverts towards the issues related to the implementations and stable usage of e-government. One important factor in providing information security to the process of e-government is the effectiveness of existing laws and policies. Thus, the participating citizens and the IT specialists were asked in the survey about this effectiveness. Following is a summary of their responses.

Table 4. 5: Frequency Distribution of Effectiveness of Existing Laws and Policies

Effectiveness of Existing Laws and Policies

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	111	22.22	22.22	22.22
	Disagree	194	38.89	38.89	61.11
	I don't know	176	35.19	35.19	96.3
	Other	19	3.7	3.7	100
	Total	500	100	100	

The participants were asked, do you think the existing laws and policies of the government make e-government applications safe? As this is ability of the existing laws and policies to protect e-government applications are their effectiveness, the responses can fulfill the objective. Majority of the participating citizens and specialists (38.89%) denied the effectiveness of legislations and policies. Only 22.22% affirmed the effectiveness while 35.19% remained indifferent as they said ‘I don’t know’. The responses of remaining 3.7% participants revealed some other views including, ‘to some extent’ and ‘most of the time’. To understand the channels through which information security threatens the e-government services, the participants were asked for the level of education, training, and awareness among the government employees whose discussion is as follows:

Table 4. 6: Frequency Distribution of Lack of Education, Training and Awareness

Lack of Education, Training and Awareness

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	445	89.09	89.09	89.09
	Disagree	18	3.64	3.64	92.73
	I don't know	27	5.45	5.45	98.18
	Other	9	1.82	1.82	100
	Total	500	100	100	

Apart from laws and policies, abilities and skills of the users is also a major factor behind secure e-services. Thus, the next question in the questionnaire survey asked the participants, do you think there is lack of education, training, and awareness for staff about information security? Most of the participating citizens and specialists (89.09%) affirmed the lack of adequate education, training, and awareness for the staff of information technology. Those who denied any such lack comprised of only 3.64% of the participants. Though there is always need of development in every field of the public management, the skills of staff can remain adequate throughout the time of development. Contrary, the result shows that the skill of the staff of information security in Saudi Arabia is lacking the adequate requisite skills. As it is seen previously the participants perceive the existing laws and policies ineffective, they were further asked if modification is required in the rules and regulations. Following is the summarized result of their responses.

Table 4. 7: Frequency Distribution of Modifications Required in Rules and Regulations

Modifications Required in Rules and Regulations

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	327	65.45	65.45	65.45
	Disagree	0	0	0	65.45

	I don't know	173	34.55	34.55	100
	Other	0	0	0	100
	Total	500	100	100	

A large majority, 65.45%, agreed that there is a need to modify the required rules and regulations. No one denied that rules and regulation of information security in the e-government of Saudi Arabia is not required to be modified. Thus, so far, the results have revealed three those areas that can affect the condition of information security in the e-services of e-government in Saudi Arabia. These three areas are the laws and policies, the education, training, and awareness, and the rules and regulation. The three areas are regarded as part of the policy framework intangible areas. A tangible area affecting the condition of information security in Saudi Arabia is the infrastructure of IT. Thus, the next question asked the respondents if the existing IT infrastructure in Saudi Arabian e-government is sufficient to secure the services. Following are the results for this question.

Table 4. 8: Frequency Distribution of Sufficient IT Infrastructure

Sufficient IT Infrastructure

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	73	14.55	14.55	14.55
	Disagree	218	43.64	43.64	58.19
	I don't know	200	40	40	98.19
	Other	9	1.82	1.82	100
	Total	500	100	100	

In answer of the question, do you think that the IT infrastructure is sufficient to secure e-government services? Most of the participants (43.64%) disagreed. Only 14.55% participating citizens and specialists said that the existing IT infrastructure is sufficient. Moreover, 40% of the participants remained indifferent as they chose the option ‘I don’t know’ and 1.82% provided other responses including the names of infrastructure components that are sufficient and not sufficient. Thus, apart intangible development of the information security in Saudi Arabia, tangible development is also required as perceived by the respondents. The participants were further asked for the effectiveness of the current security policy in Saudi Arabia.

Table 4. 9: Frequency Distribution of Effectiveness of Current Security Policy

Effectiveness of Current Security Policy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	200	40	40	40
	Disagree	73	14.55	14.55	54.55
	I don't know	218	43.64	43.64	98.19
	Other	9	1.82	1.82	100
	Total	500	100	100	

Current security policy for information shared via applications of e-government is a matter of ambiguity. This is evident for the above table, which shows that most of the citizens and specialists (43.63%) remained indifferent and 14.55% disagree that the current security policies are effective. On the other hand, 40% of the participants considered these security policies effective. The reaming 1.82% participants gave other responses. Moreover, the participants were asked for the security of e-government applications and their responses are summarized as follows.

Table 4. 10: Frequency Distribution of Good Information Security

Good Information Security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	209	41.82	41.82	41.82
	Disagree	145	29.09	29.09	70.91
	I don't know	136	27.27	27.27	98.18
	Other	9	1.82	1.82	100
	Total	500	100	100	

Most of the participating citizens and specialists (approximately 42%) agreed in answer of the question do you think that information security is good enough in e-government application. From the respondents, those who disagreed, remained indifferent, and provided other responses comprised of 29.09%, 27.27%, and 1.82% respectively. Positive perception of the people regarding the security of the e-government application in Saudi Arabia follows the reasons as perceived by them in the previous questions. It can be said that the information security of the application is good because of ineffective laws and policies. After realizing the condition of information security and the possible reasons behind it, the next question in the questionnaire aimed at determining the possible solutions.

Table 4. 11: Frequency Distribution of Reduction in Vulnerability through Increased Awareness

Reduction in Vulnerability through Increased Awareness

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	400	80	80	80
	Disagree	36	7.27	7.27	87.27
	I don't know	64	12.73	12.73	100
	Other	0	0	0	100
	Total	500	100	100	

The next question asked the participants do you think increased awareness of citizens will reduce the vulnerabilities for e-government. Although a majority of the participants (80%) agreed in this question, considerable percentage of participants (7.27%) denied too. While 12.73% of the participants remained indifferent. The participants were further asked if numerous sources threaten the information security of the e-government applications. Following are their summarized responses.

Table 4. 12: Frequency Distribution of Threat from Variety of Sources

Threat from Variety of Sources

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	443	88.68	88.68	88.68
	Disagree	28	5.66	5.66	94.34
	I don't know	19	3.77	3.77	98.11
	Other	9	1.89	1.89	100
	Total	500	100	100	

As expected, threats to the information security from a variety of the sources are affirmed by the majority (88.68%). Moreover, 5.66% disagreed in response of the question that do you find that the current security policy in securing government services is effective. Approximately 3.77% of the participants said 'I don't know' while only 1.89% given other responses including 'external threats only' and 'may be'. To elaborate the sources of threats, last question of the study presented a list of potential sources of threats in front of the participants. They were asked to mark the source they think is the most influential type of threat are facing e-government.

Table 4. 13: Frequency Distribution of Sources of Threats to E-Government

Threats to E-Govt.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Accidents	28	5.66	5.66	5.66
	Software Errors	123	24.53	24.53	30.19
	Hardware Failures	28	5.66	5.66	35.85
	Environmental Influences	19	3.77	3.77	39.62
	Hacktivists	160	32.08	32.08	71.7
	Terrorists	75	15.09	15.09	86.79
	Government Intrusion	19	3.77	3.77	90.56
	Foreign Nation States	9	1.89	1.89	92.45
	Organized Crime	38	7.55	7.55	100
	Other	0	0	0	
	Total	500	100	100	

The least chosen threat includes environmental influence, government intrusion, and foreign state notations comprising of 3.77%, 3.77% and 1.89% only. Most of the respondents (32.08%) considered hacktivists the most influential threat to the information security. Other frequently chosen threats included software errors (24.53%) and terrorists (15.09%). A better comparison the threats to information security in Saudi Arabia is illustrated in the following pie chart.

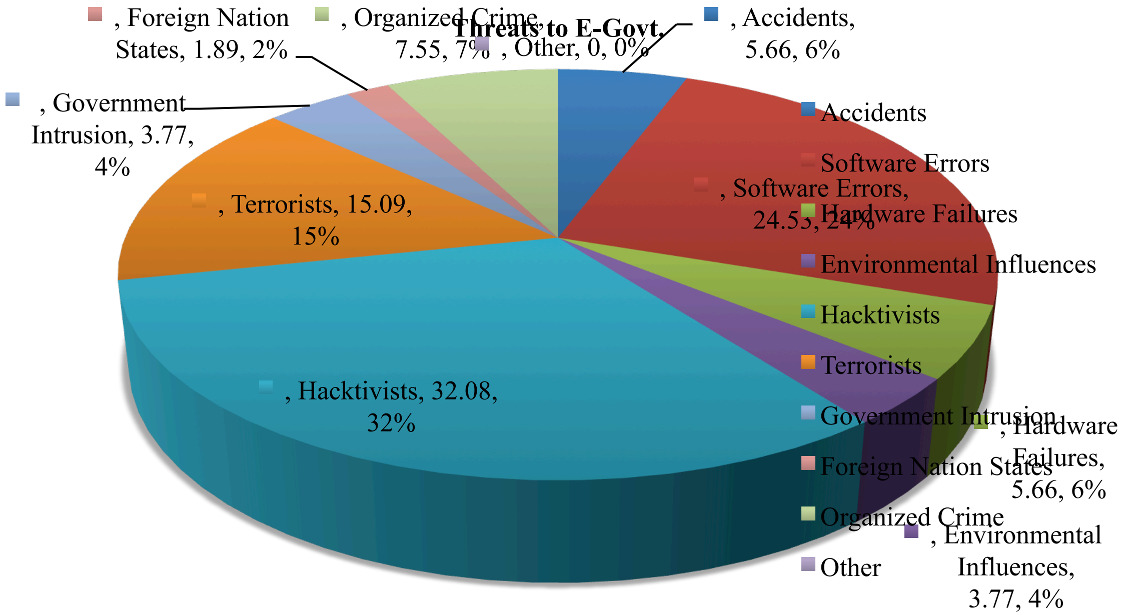

Figure 4. 1: Pie Chart for Threats to the E-Government

Other than the comparison of the threats to the information security, a comparison between frequencies of agreed and disagreed participants for different questions is illustrated in the following clustered bar graph. It can be seen that the most agreed upon factor are threats from a variety of sources, reduction in vulnerability through increased awareness, modifications required in rules and regulations, lack of education and awareness, and usefulness and effectiveness of e-government. More than 50% participants agreed for each of these factors. The least agreed factors include sufficient IT infrastructure and effectiveness of existing laws and policies.

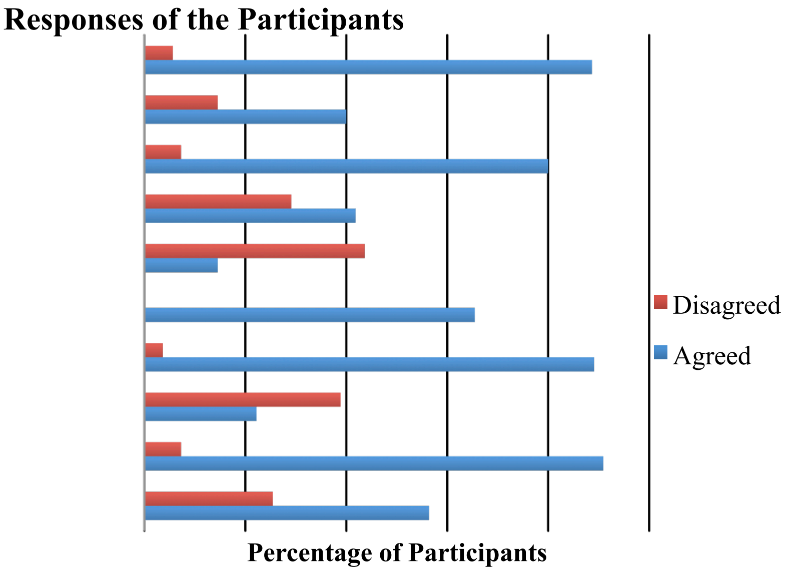

Figure 4. 2: Clustered Bar Graph for Responses of the Participants

4.3 Interview Results

The survey results revealed many organizational and technical factors that influence the effectiveness, vulnerabilities, and threats to e-services of the e-government in Saudi Arabia. These factors are discussed in this section in light of the findings from the interview result.

4.3.1 Technological Issues

The concept of technological issues in information security can be as lows as "setting technical standards", vendor's challenges", "viruses and worms", "maintaining a high level performance", and "troubleshooting" [34]. Such issues are not possible to be eliminated but can be reduced. On the other hand, there can be high issues that affect the information security in broader aspect. Fortunately, the ICT specialists included in the interview panel identified some of the high-level security issues associated with IT standards and national information and communication technology infrastructure (NICT). A pictorial representation of these issues is illustrated as follows:

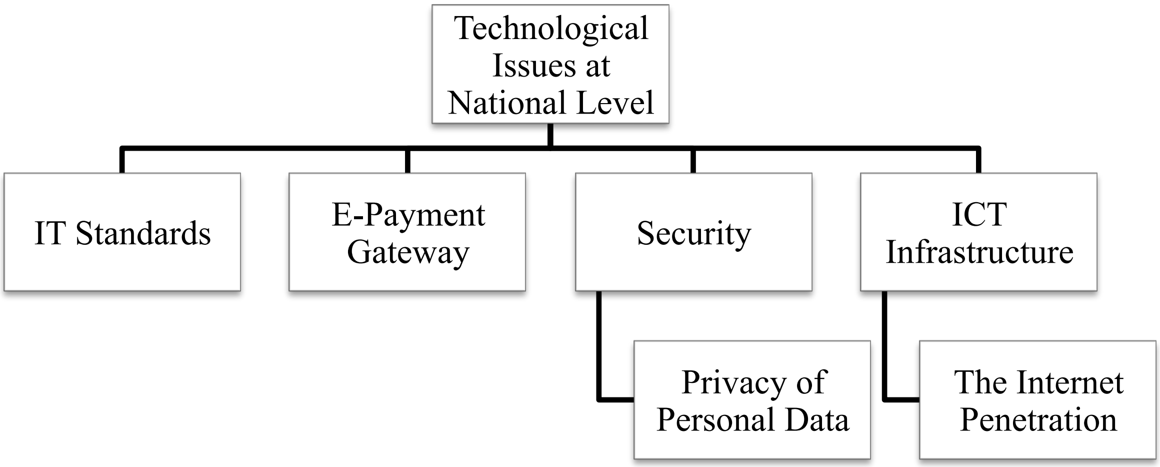

Figure 4. 3: Technological Issues at National Level

4.3.2 Insufficient IT Infrastructure

Fig. 4.3 indicates that 43.64% participants consider that IT infrastructures are not sufficient. Diffusion and implementation of an e-government significantly depends on IT infrastructure that comprise of services and networks [33]. A sufficient IT infrastructure can ensure the time and effort saving of the employees facilitating them in using the technology for daily tasks, as the government agencies are able to share work, interact, and cooperate. However, IT infrastructure is still lacking in the organizations of Saudi Arabia. Thus, the public service providers must give high priority to the provision of IT infrastructure. The need of such priority is reflected in the response of an interviewee, “each employee in our organization has copies of files. There are many systems at certain layers that are not connected, and copying the files for accessing them consumes the virtual space." Another employee criticized the existing IT infrastructure saying, "I work on a ten year old infrastructure and the service is not up-to-date with the current requirements. How can we make assure that the services are saved while may are out of reach and have no sufficient facilities to avail the services." Thus, for secure participation of the private sectors, citizens, organizations, and agencies upgrading the current ICT structure to make it modern and standardized is very important. The importance of integrating a sound ICT structure across governmental organizations is emphasized in the literature too.

4.3.3 Privacy and Trust in E-Services of E-Government

Issue of security of the e-government all over the world is emphasized in national and international publications. Results of the questionnaire survey also revealed that the citizens in Saudi Arabia do not consider the current practices of e-government safe for information shared via electronic services. Interviewees were also asked about their level of trust in the e-services when they share their personal and confidential information such as name, date of birth, details of credit card, and ID number. The interviewees are found afraid of the threats posed to their information shred on websites. They think that the websites of government services are not safe enough and even if they are, the users are not communicated with the surety. The fears include that the information shared online might get exposed or destroyed due to lack of security. One citizen in the interview panel was not even in favor of sharing information electronically saying, "I do not trust in sharing my information on internet neither I am interested in getting things while sitting in my home. If I need anything, I'll go and will take it hand by hand." In sharing the threats, one interviewee shared a friend's case as, "my friend's experience made me reluctant in sharing my information on internet. He used his visa card to purchase a laptop but the website was fraud and he lost money and got nothing. I cannot trust any service whether it is privately owned or publically owned." Reponses of other interviewees showed further issues of security including electronic crime, Trojans, spam, hackers, and viruses.

4.3.4 Laws and Legislation

Rights of e-services users are not preserved until the legislation is strong. Laws and policies of a country are backbone to the information security of the e-government applications, which can cover the issues of computer crime and electronic signature laws. Moreover, accommodation of e-services requirement needs compatibility of existing statues with the new laws. In addition, the awareness of the modified and newly approved legislation among the citizen is part of the structure. According to one specialist in the interview panel, "only introducing laws and regulation according to the changing requirement of information security is not enough. Two sub-factors fuel the success of new legislations. One is the awareness among the officials and the citizens and other is training the staff of the law enforcement agency for implementation of the new legislation." One of the interviewees is an IT manager and member of the task force of e-government who explained, "The government will be required to amend its existing laws and establish an e-business infrastructure by involving the banking system and other financial institutions as part of securing the e-government applications." Realizing the issue of information security, the Saudi government has developed the electronic services laws.

4.3.5 Security

The information dealt by the e-government is confidential and highly sensitive; therefore, protection of the information from internet criminals and hackers is crucial. E-transaction is an important feature of e-government services and the most sensitive one in terms of security. The security threats to this feature are sever if a criminal is able to alter and intercept data during transaction and steal valuable information. According to Fulford and Dohetry [35], "in order to retain the availability, confidentiality, and integrity of the all the information embedded in the ICT, adequate control and security procedures are introduced."

Findings of the current research also emphasized the need to introduce such procedures in Saudi Arabia given large exchange of confidential information via internet. The participant of the study also emphasized o the need to secure their shared information while they use e-services. One of the IT specialist in the interview panel said, "A high level of security is ever crucial nowadays as internet has become the primary source in performing business transactions, interacting with other people, and exchanging information. Also, not it is used by military and government establishment in Saudi Arabia making the issue of security more sensitive."

4.3.6 Public Key Infrastructure

Citizens and officials in Saudi Arabia realize that security is not only important but also its provision ensures penetration of e-service usage among the citizens of Saudi Arabia. The issue of security in the e-government national project in Saudi Arabia is common in other developed and developing country too. As one of the official said, "Major challenges that we face in implementing e-government in Saudi Arabia are building payment gateways and developing a security infrastructure. So far, the measures taken include introducing smart cards and building a public key infrastructure and secure payment gateway." Therefore, longer security infrastructure of e-government in Saudi Arabia requires establishing specific aims. Two milestones are achieved by the government in this context. First is the selection of a public key infrastructure by the government of Saudi Arabia for its e-government project. One of the officials in the interview panel emphasized the benefit of selecting public key infrastructure and said, "The information, privacy and security, without the use of public keys, will be highly compromised." Findings of the current research identified the following main elements:

- Electronic Signature: through electronic signature, the documents to be exchanged electronically can be signed through digital encryption technology. Consequently, the intended receiver is able to validate the signature.
- Data Integrity: This includes the ability to detect partial deletion, alteration, or modification in the data after it is sent.
- Authentication: it enables to identify a person in a definite way.
- Confidentiality: making sure that no one other than the authorized individual is able to read or understand the information exchanged.

Thus, usage of public key infrastructure is mentioned by almost all the officials in the interview panel. Participants mentioned the benefits of securing email messages and protecting websites via authenticating the access using a public key. Moreover, the use of electronic signature can not only secure the transactions but also it can be added to forms, messages, and documents for authenticity. Apart from human beings, inter-computer safety is also mentioned by some of the ICT specialists. The possible ways to ensure a secure interaction between computers, as suggested by the interviewees, computers can also use digital signature produced on their own. Moreover, obtaining the exact official transaction time and attaching it to the transaction can work as a timestamp for correspondence and documents.

Although the need of security functions is realized by the practitioners of e-government, its complexity is the most influential obstacle in its implementation. In every country, with or without e-government, information security has been an important issue since the widespread use of the Web. Its nature of being in reach of everyone makes its security harder than that of the other mediums of information exchange. Despite numerous advancements in technological procedures for interment security, it is not possible to eliminate each and every potential threat. What can be done is to assure that the available security measures are implemented in Saudi Arabia to make the use of e-services foolproof. Authenticating the usage of e-services in the country can make the services password protected after assigning the users with ID's and passwords. Another measure, which is the simplest so far, is to using digital signature. Through its use, the chances of someone's false claims over exchanged information and the chances of alteration in the messages can be minimized. One of the Saudi officials in the interview panel explained the public key infrastructure as, "It is a structure that builds an environment of trust for transactions conducted over public networks to build up a framework for issuing certificates to be used for the creation of original documents, access control, digital signatures, authentication, integrity, and confidentiality among others."

From face-to-face interview session with the officials, the solution to information security issue is found to be developing and modifying the public key infrastructure. The benefits that the interviewee discussed include surety that an internet document is original, ability of an individual to sign online a contract, making the right websites accessible while blocking the unsafe content, and letting people communicate online without the fear of intrusion. In addition, the organizational processes including renewal of driving license and identification of customers of bank in order to manage traffic are also the benefits of developing a public key infrastructure.

Since January 2007, Saudi government has accomplished several tasks related to the information security of e-government applications. The accomplishments include a number of training, conference, and awareness programs, using internet for payments of public transactions, embedding a government e-procurement system, drafting a certification policy, a digital signature law, and other accomplished and ongoing projects of public key infrastructure. Many of the interviewees mentioned these measures; however, the potential pitfalls cannot be neglected. Specifically the cultural and structural obstacles such as difficulties that the citizens and employees face in understanding technical issues, high costs involved in the development procedure, lacking support to the programs of public key infrastructure, and weak training and education of the employees regarding their development for technical acceptance.

Thus, once a sound security infrastructure is in place access it will accelerate the availability and access to the e-services as people’s trust in using e-services is subject to the security infrastructure. However, once it is implemented, upgrading continually is an ongoing task of the implementers. This is because complete elimination of the threats can never be guaranteed as the medium of exchange in e-government is internet which is in reach if everyone. Any IT project whether as broad as e-government or as narrow as automation of an organization, continually face the issue of security. For the case of e-government, information security becomes more sensitive given the nature of information going electronic in the project such as government classified information and profiles of officials and citizens. Therefore, incorporating advanced security is a priority is the e-government system to ensure at every level of the public information infrastructure the protection against vulnerabilities and fraud.

4.3.7 Privacy of Personal Data

Interviewees including the citizens and the officials aggraded upon the provision of privacy of information that users share on e-government applications. Given the above realization of widespread security issue, privacy of personal data is indeed an important concern of the e-services users. For example, one interviewee said, “I believe in signature as an important means of authentication of information. With electronic information, such as models, letters, documents, how it can include signature.” It is found in the current study that access to personal information of the users that is identifiable must be limited. Other measures that interviewees suggested for privacy of personal data include, making the users aware of the privacy issues and communicating them with the terms in advance before they provide personal information, limiting the required personal information of the users and removing the fields of unnecessary information from the online forms, improving the awareness of ethical considerations of privacy among the employees handling e-government applications, and limiting the number of authorized individuals who are allowed to access personal data of the users.

An important factor behind the fear of privacy is the lack of trust in Saudi citizens within the e-government applications. For instance, sharing the personal data on internet is associated with confidentiality. Some private organizations follow strict practices of securing the data and information. However, need of such practices in e-government of Saudi Arabia is ever crucial given high chances of intrusion and misuse of the database that holds confidential personal information of citizens. According to an official, “I consider the need of four critical aspects for making citizens able to engage in electronic business: A systematic integrated infrastructure of laws and regulations, electronic payment system for financial exchange, public key infrastructure for safe environment, and communication infrastructure."

A review of concerned documents regarding Saudi project, a list of organizations is obtained that are responsible for security matter in the country. Following table illustrated the list of organizations and their responsibility.

Table 4. 14: Roles of organizations responsible for security in Saudi Arabia

Organization	**Tasks**
Chambers of Commerce	Business development gate
Centre ratification	For monetary institutions, communications companies and companies such as Aramco
Ministry of Culture and Information	The inclusion of intellectual property rights in electronic dealing
Ministry of the Interior	Preparation of information security and systems privacy
Ministry of Finance	Government procurement systems
Ministry of Trade and Industry	Work on the development of regulations for electronic commerce
Saudi Communications Company	Processing the communications Infrastructure
Electronic communications and information technology	Development of a system for electronic dealing
Ministry of Communications and Information Technology	Supervision of the Standing Committee on electronic dealing
King Abdul Aziz City for Science and Technology	Some necessary regulations for the ratification of digital information including the establishment and operation of the National Centre

Interview results revealed that an integrated security system of public keys help the Saudi government in dealing the information security in a suitable environment. This can be viewed as a system for managing encryption keys using digital certificates. According to the National Centre for Digital Certification in Saudi Arabia, the digital certificate achieves the following key objectives:

- Enabling the recipient to verify electronic signature authenticity on a document
- Detecting the attempts to alter data exchanged online for safety of the information

- Ensuring the confidentiality of the exchanged information keeping the information in such a form that the handler can understand the nature
- Enabling the users and service providers to identify conclusive identity of each other.

4.4 Summary of the Chapter

The responses show the provision of e-services in Saudi Arabia by e-government is not flawless and the users face concerns while availing the facility. Citizens and the IT specialists in Saudi Arabia consider the adoption e-government important for the benefit of citizens. One important factor in providing information security to the process of e-government is the effectiveness of existing laws and policies. Majority of the respondents affirmed that the existing laws and policies of the government make e-government applications unsafe. The channels through which information security threatens the e-government services include lack of education, training, and awareness for staff about information security. Though there is always need of development in every field of the public management, the skills of staff can remain adequate throughout the time of development. Contrary, the result shows that the skill of the staff of information security in Saudi Arabia is lacking the adequate requisite skills. The results have revealed that two areas affect the condition of information security in the e-services of e-government in Saudi Arabia. These two areas are the education, training, and awareness and the rules and regulation. The two areas are regarded as part of the policy framework intangible areas. A tangible area affecting the condition of information security in Saudi Arabia is the infrastructure of IT. However, apart intangible development of the information security in Saudi Arabia, tangible development is also required as perceived by the respondents. Moreover, current security policy for information shared via applications of e-government is a matter of dissatisfaction. Negative perception of the people regarding the security of the e-government application in Saudi Arabia follows the reasons as perceived by them. It can be said that the information security of the application is not good because of lack of education, training, and development and insufficient IT infrastructure. Further responses showed that several factors other than increased awareness could reduce the vulnerability for the e-government. The most influential threats to the information security of Saudi Arabian e-government include hacktivists, software errors and terrorists. On the other hand, the least influential threats include environmental influence, government intrusion, and foreign state notations.

From face-to-face interview session with the officials, the solution to information security issue is found to be developing and modifying the public key infrastructure. The benefits that the interviewee discussed include surety that an internet document is original, ability of an individual to sign online a contract, making the right websites accessible while blocking the unsafe content, and letting people communicate online without the fear of intrusion. Measures that interviewees suggested for privacy of personal data include, making the users aware of the privacy issues and communicating them with the terms in advance before they provide personal information, limiting the required personal information of the users and removing the fields of unnecessary information from the online forms, improving the awareness of ethical considerations of privacy among the employees handling e-government applications, and limiting the number of authorized individuals who are allowed to access personal data of the users.

CHAPTER 05: CONCLUSION

5.1 Overview of the Study

In many countries, the implementation of the E-Government has proved to be useful in providing efficient services to the consumers. This increases the speed of the work and does not cause any unnecessary delays. All these aspects matters for the efficient service of the Government work. In the end, it proves to be beneficial for both Government and the citizens living in Saudi Arabia. Therefore, in this study, all the issues related to the Information Security Policy will be discussed in detail. The research study is worth for a number of reasons. Firstly, it will help in assessing the degree of effectiveness of the present security policy, security holes in the policy, and threats not addressed by the policy. It, in turn, would help in coming up with measures of ensuring that the policy is security-oriented, which increases citizens' confidence in using e-government services. The literature review revealed that in Saudi Arabia, there is the absence of agencies to monitor the accountability of e-government services. Most of the workers of offices in Saudi Arabia lack professionalism, and this is a great weakness in the implementation of appropriate policy for e-government. In order for the government to solve this problem, it needs to restructure these rules and regulations to attain online transactions that are more democratic and transparent. In order to have an effective and efficient implementation of the e-government program, there must be qualified personnel to perform such a task. The absence of such staff in Saudi Arabia poses a major challenge to the IT policy. The government of Saudi Arabia should come up with highly training programs in addition to sufficient number of IT specialists. The research method for this study uses inductive approach and a mixed design following the philosophy of positivism of case study. Data for the case of Saudi Arabia is collected via primary source and the instruments are questionnaire survey (quantitative part) and face-to-face interview (qualitative part). Quantitative data analysis includes frequency distribution, clustered bar graphs, and pie charts. Analysis of qualitative data is a three-step process that includes reducing the data, displaying the data, and verifying or drawing conclusion.

5.2 Findings

Diffusion and implementation of an e-government significantly depends on IT infrastructure that comprise of services and networks [33]. A sufficient IT infrastructure can ensure the time and effort saving of the employees facilitating them in using the technology for daily tasks, as the government agencies are able to share work, interact, and cooperate. However, IT infrastructure is still lacking in the organizations of Saudi Arabia. The responses show the provision of e-services in Saudi Arabia by e-government is not flawless and the users face concerns while availing the facility. Citizens and the IT specialists in Saudi Arabia consider the adoption e-government important for the benefit of citizens. One important factor in providing information security to the process of e-government is the effectiveness of existing laws and policies. Majority of the respondents affirmed that the existing laws and policies of the government make e-government applications safe. The channels through which information security threatens the e-government services include lack of education, training, and awareness for staff about information security. Though there is always need of development in every field of the public management, the skills of staff can remain adequate throughout the time of development. Contrary, the result shows that the skill of the staff of information security in Saudi Arabia is lacking the adequate requisite skills. The results have revealed that two areas affect the condition of information security in the e-services of e-government in Saudi Arabia. These two areas are the education, training, and awareness and the rules and regulation. The two areas are regarded as part of the policy framework intangible areas. A tangible area affecting the condition of information security in Saudi Arabia is the infrastructure of IT. However, apart intangible development of the information security in Saudi Arabia, tangible development is also required as perceived by the respondents. Moreover, current security policy for information shared via applications of e-government is a matter of dissatisfaction. Negative perception of the people regarding the security of the e-government application in Saudi Arabia follows the reasons as perceived by them. It can be said that the information security of the application is not good because of lack of education, training, and development and insufficient IT infrastructure. Further responses showed that several factors other than increased awareness could reduce the vulnerability for the e-government. The most influential threats to the information security of Saudi Arabian e-government include hacktivists, software errors and terrorists. On the other hand, the least influential threats include environmental influence, government intrusion, and foreign state notations.

From face-to-face interview session with the officials, the solution to information security issue is found to be developing and modifying the public key infrastructure. The benefits that the interviewee discussed include surety that an internet document is original, ability of an individual to sign online a contract, making the right websites accessible while blocking the unsafe content, and letting people communicate online without the fear of intrusion. Measures that interviewees suggested for privacy of personal data include, making the users aware of the privacy issues and communicating them with the terms in advance before they provide personal information, limiting the required personal information of the users and removing the fields of unnecessary information from the online forms, improving the awareness of ethical considerations of privacy among the employees handling e-government applications, and limiting the number of authorized individuals who are allowed to access personal data of the users.

5.3 Implications and Recommendations

The current study has identified those organizational and technological issues that affect the information security in Saudi Arabia at national level. Moreover, many areas are highlighted where modifications can make the practice of e-government safer. The measures taken by Saudi government in developing organizations are far admired than the cultural development. Lack of awareness in the citizens and inadequate training of the employees dealing with e-services is not satisfactory. Moreover, the most advancing measures taken to reduce security threats of information shared via internet are infrastructure development. However, it needs to be updated regularly as the challenges to information security are always changing. Despite all the attempts to ensure information security in e-government of Saudi Arabia, trust of the citizens in the applications is still low. Thus, Saudi government must given priority to the awareness programs.

It should be stressed that the purpose of e-government is not only to increase the level of computerization of government structures. It refers to the transformation of the essence of government operations. The structure of relations with citizens and business units are expected to change. Thus, the program will fulfill the valuable social function. In this way, the method of delivering public services will be significantly transformed. It is expected that relationships of partnership between citizens and the government may prevail. Moreover, the scope for corruption is expected to be reduced, as new forms of control will emerge. As corruption constitutes significant obstacles for sustainable development, e-government may minimize this problem.

REFERENCES

[1] N. Adam, O. Dogramaci and A. Gangopdhyay, Electronic commerce technical business and legal issues. New Jersey: Prentice Hall PIR, 1999.

[2] M. Ahmad al. (2012). Saudi Arabia emerging as leader in e-government. [Online]. Availbale FTP: http://al-shorfa.com/en_GB/articles/meii/features/2012/09/26/feature-01

[3] G. Aichholzer and R. Schmutzer, (2000) “Organizational challenges to the development of electronic government”, DEXA 2000, IEEE Press, 2000, pp. 379-383.

[4] I. Al-Furaih, (2002) “Internet regulations; the Saudi Arabian experience”. The Internet Society's 12th Annual INET Conference: Internet Crossroads: Where Technology and Policy Intersect.

[5] A. Almogbil, Security. (2005) Perceptions and practices: Challenges facing adoption of online banking in Saudi Arabia. Ph.D. Dissertation. The George Washington University.

[6] F. Alyabis, F. (2000) Examining the impact of Internet electronic commerce on commercial organizations in Saudi Arabia. Ph.D. Dissertation. University of Northern IOWA.

[7] D.B. Cabello and U.K. Ravula U.K., (2006), Public E-services toward citizens. Lulea University of technology, 2006.

[8] E-Commerce: Impacts and policy challenges. (2000) Organization for Economic Co-operation and Development, OECD Economic On-look.

[9] A. Zahlan, (1999). Arabs and the challenges of science and technology: Progress without change. Beirut: Centre for Arab Unity Studies (CAUS).

[10] L. Fredricks. (2007). The e-government program of Saudi Arabia: Advantages and challenges. Retrieved from http://workspace.unpan.org/sites/internet/Documents/UNPAN033485.pdf

[11] O. Al-Mushayt, K. Haq, & Y. Perwej. (2009). Electronic government in Saudi Arabia: A positive revolution in the peninsula. International Transactions in Applied Sciences, 1(1), pp. 87-98.

[12] K. Layne, & J. Lee. (2001). Developing fully functional e-government: A four stage model. Government Information Quarterly, 18, pp. 122-136.

[13] I. Nadi. (2013). Influence of culture on e-government acceptance in Saudi Arabia. Retrived from http://arxiv.org/ftp/arxiv/papers/1307/1307.7141.pdf

[14] http://www.eSurveysPro.com/Survey.aspx?id=0ed8beda-696e-4e7b-8646-27c43b31b872

[15] Ornstein, M. D. (1998) Survey Research, Current Sociology, Vol. 46, No. 4, pp. 3-136

[16] Lewis, P. and Thornhill, A. (2003) Research Methods for Business, Pitman

[17] Myers, M D (1997), Qualitative research in information systems, Management Information Systems Quarterly, 21, 241-242.

[18] Miller. W. (1996) A Working Definition for Total Quality Management. Journal of Quality Management.1, 149-159.

[19] Punch, M. (2005) Introduction To Social Research: Qualitative And Quantitative Approaches, London: Sage

[20] Silverman, D. (1997) Qualitative Research: Theory, Method and Practice, Sage

[21] Miles, Matthew B. and A. Michael Huberman (1994), Qualitative Data Analysis: A New Sourcebook of Methods, Beverly Hills, CA: Sage.

[22] Lazo. F. (2010) An Overview of Qualitative and Quantitative Method. National Center for Atmospheric Research.

[23] Bryman. A (2006) Integrating Quantitative and Qualitative: how is it done? SAGE Publications, London,6(1), 97-113.

[24] Ahmed, U. (2011) Factors affecting time and cost performance on large construction projects in Libya, MSc thesis submitted to Heriot Watt University.

[25] Locke, K.(2001) ,Grounded Theory in Management Research in Bryman, A. and Bell, E. (2007).Business research methods. Oxford University Press.pp.578-600.

[26] Spiggle, S. (1994). Analysis and Interpretation of Qualitative Data in Consumer Research .Journal of Consumer Research. 21(3), 491

[27] Ragin, C.C. (1997) 'Turning the tables : how case-oriented methods challenge variable-oriented methods' Comparative Social Research 16: 27–42

[28] Myers, M. D. (2009). 'Qualitative Research in Business & Management'. Sage, London

[29] Strauss, A., & Corbin, J. (1990). Basics of qualitative research: Grounded theory procedures and techniques. Newbury Park, CA: Sage.

[30] Strauss, A. (1987). Qualitative analysis for social scientists. Cambridge, UK: Cambridge University Press.

[31] David Silverman (1993). "Beginning Research". Interpreting Qualitative Data. Methods for Analysing Talk,. Text and Interaction. Londres: Sage Publications.

[32] Patel R, & Davidsson, B. (2003) Forskningmetodikens grunder- Att planera, genomföra och rapportera en undersökning, Studentlitteratur, Lund.

[33] Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. Government Information Quarterly, 18, 122 -136

[34] Ndou , V. (2004). E-government for developing countries: opportunities and challenges. The Electronic Journal on Information Systems in Developing Countries, 18, 1, 1-24

[35] Fulford, H. and Doherty, N.F., (2003). The application of information security policies in large UK-based organizations: an exploratory investigation. Information Management and Computer Security, 11(3), pp. 106-114.