REFERENCE

MULTI-STAKEHOLDER ENQUIRY FOR SECURING E-BUSINESS ENVIRONMENTS: A SOCIO-TECHNICAL SECURITY FRAMEWORK

JA'FAR S. ALQATAWNA

A thesis submitted in partial fulfilment of the requirements of
Sheffield Hallam University
for the degree of Doctor of Philosophy

October 2010

"Allah will exalt in degree those of you who believe and those who have been granted knowledge. And Allah is well-acquainted with what you do"

Holy Quran Chapter 58. Verse 11

"Whoever takes a path in search for knowledge, Allah will facilitate for him a path to Paradise"

Prophet Mohammad's Teachings

Cryptography is a branch of mathematics. And like all mathematics, it involves numbers, equations, and logic. Security, palpable security that you or I might find useful in our lives, involves people: things people know, relationships between people, people and how they relate to machines. Digital security involves computers: complex, unstable, buggy computers. Mathematics is perfect; reality is subjective. Mathematics is defined; computers are ornery. Mathematics is logical; people are erratic, capricious, and barely comprehensible. The error of Applied Cryptography is that I didn't talk at all about the context. I talked about cryptography as if it were The Answer™. I was pretty naive...If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

Bruce Schneier (2000): Secrets & Lies.

Abstract

Increasing the security of e-Business is best achieved by considering the environment in which e-Business applications need to be implemented and used; this implies that e-Business should be viewed as a complex socio-technical system with three interconnected and interacting elements: stakeholders, enabling technology, and business processes. This multiple perspective has rarely been captured by previous studies of e-Business security which perceive security from a narrow, single-sided technical view. This thesis argues that the predominant technical security approaches consider neither the multifaceted nature of e-Business security nor the requirements and influences of the various stakeholders involved in its context. In Jordan e-Business adoption is still in its early stages and is gaining the attention of several parties. Therefore, the primary approach in this research is an interpretive stakeholder analysis in which notions of a socio-technical perspective are employed as required in order to develop a conceptual framework for better understanding of e-Business security in the context of Jordan. In other words, an interpretive approach has been adopted as a mean of inquiry aiming at developing a holistic understanding of e-Business security in relation to its context as well as considering all the stakeholders in the problem area. This methodological choice was influenced by three factors: the nature of the research problem, the researcher's theoretical lens, and the degree of uncertainty in the study environment. Consequently, four major stakeholders were identified and their security implications were explored. The study's findings provide rich insights into the security of e-Business by identifying and interpreting the roles, the perceptions, and the interactions of several groups of security stakeholders. The theoretical contributions include: an explanatory framework of organisational, legal, human and technical factors affecting security in e-Business environments which was developed by employing an inductive stakeholder analysis as well as the identification of several organisational aspects, such as governance, communication, power conflict, awareness, and resistance to change, and their relationships to security as well as their practical implications at individual, organisational, and national levels. Additionally, the findings provide insights into the customers' side of the security problem and explain its relationships with other stakeholders, including government, business and technology providers. This is a sound practical contribution which can help these stakeholders to design better security approaches based on a deeper understanding of customers' security requirements.

List of Publications

ALQATAWNA, J., SIDDIQI, J., AKHGAR, B. and HJOUJ BTOUSH, M. (2010). SECURITY IN E-BUSINESS: Understanding customers perceptions and concerns. In: *The 6th International Conference on Web Information Systems and Technologies (WEBIST).* Valencia, Spain.

SIDDIQI, J., ALQATAWNA, J. and HJOUJ BTOUSH, M. (2010). Do insecure systems increase global digital divide? Book chapter in: KAMEL, S. (ed.). *Strategies for technological diffusion and Adoption: National ICT Approaches for socioeconomic development.* IGI Global.

ALQATAWNA, J., SIDDIQI, J., AKHGAR, B. and HJOUJ BTOUSH, M. (2009). E-Business security: Methodological considerations. In: *World Congress on Science, Engineering and Technology.* Dubai, UAE.

ALQATAWNA, J., SIDDIQI, J., AKHGAR, B. and HJOUJ BTOUSH, M. (2008). Towards holistic approaches to secure e-Business: A critical review. In: *The 2008 International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE'08).* Las Vegas, Nevada, USA.

ALQATAWNA, J., SIDDIQI, J., AKHGAR, B. and HJOUJ BTOUSH, M. (2008). A holistic framework for secure e-Business. In: *The 2008 International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE'08).* Las Vegas, Nevada, USA.

Acknowledgments

First and foremost, I thank Allah Almighty for giving me the power of knowledge and the opportunity to improve my qualifications and fulfil my desires.

I am heartily thankful to my supervisor, Professor Jawed Siddiqi. Without his endless support, encouragement, constructive comments and great trust in me, this work would not have been possible. I shall always be grateful to him for his moral support and tolerance throughout the course of this thesis. I also thank him for navigating this research along the thin line between practice and theory. His red ink was worth more to me than gold.

I am indebted to Prof. Louise Yngström who helped in shaping my perspective on information security. Her holistic approach inspired me and opened my eyes to the multidisciplinary nature of information security.

A special word of thanks is due to Professor Trevor Wood-Harper from The University of Manchester and Dr. Murray Clark from Sheffield Hallam University for being part of the examination committee of this thesis.

It is a pleasure also to thank my colleagues at Cultural, Communication and Computing Research Institute (C3RI) for their support and encouragement. Furthermore, I wish to extend my appreciation to all my friends, especially the Jordanian community in Sheffield, for their encouragement and valuable discussions, and for the good times we spent together.

Words are not enough to express my deepest gratitude to my parents, who through the years have provided me with endless love, support, patience and continuous encouragement.

My warmest gratitude goes to my beloved wife Fida' Al-Obaisi; her unwavering belief in me motivated me and gave me the confidence to complete this work. Without her and our dazzling daughter Jana this achievement has no meaning.

Finally, I wish to acknowledge with gratitude the financial support I have received from the University of Jordan.

Ja'far S. Alqatawna
Sheffield, 2010

Table of Contents

List of Figures

List of Tables

Chapter 1 : Research Orientation

E-Business is more than just combining business with Internet technologies. Diverse issues face organisations endeavouring to adopt e-Business to reap its potential benefits. Security of e-Business is one of the major issues facing a wide range of stakeholders including e-Business organisations, customers, governments and technology providers. Unfortunately, this issue is usually overlooked, comes as an afterthought or is perceived from a purely technical dimension, with a notable increase in the number of online security breaches such as identity theft, privacy violation, vandalism, and infringement of intellectual property rights. This gives a clear indication that traditional security approaches and ad hoc security solutions are insufficient to thwart this dramatic increase in security breaches. These approaches, which perceive security from one dimension, seem unable to provide adequate security levels for today's business environment. This encourages us to change our way of thinking and investigate other approaches that perceive security as an integrated part of business in the first place and then follow a holistic way of understanding and solving the e-Business security problem.

This thesis is concerned with information security within e-Business environments. It views e-Business systems as interconnecting and interacting components (people, software, hardware, procedures and data) and Information System (IS) with a technological infrastructure and organisational framework, rather than as a purely technological infrastructure (Katsikas at al., 2005). It argues that the predominant technical security approaches do not consider the multifaceted nature of e-Business security nor the requirements and influences of the various stakeholders involved in its context. Therefore, it devises an interpretive stakeholder analysis with a socio-technical framework of inquiry, used to support the research design and outcomes. This will assist in developing a better understanding of e-Business security in the context of Jordan, where e-Business adoption, still in its early stages, is gaining the attention of several parties.

This chapter provides a background to the problem situation; it sets the scene of e-Business security in the context of the study and identifies the research gap that is intended to be

filled by the proposed study. Additionally, it outlines the research's aims, objectives and contributions, and then introduces the rest of this thesis.

1.1 Problem Situation and Research Gap

Jordan has experienced a technological evolution which started during the nineties and continues until today (Al Nagi & Hamdan, 2009; Al-Jaghoub & Westrup, 2003). This means ICT plays a significant role in the Jordanian economy. A rapid development in several ICT sectors is notable (ESCWA, 2005). One aspect of this development is the adoption of e-Business by a number of local companies which have started to provide more advanced electronic services that utilise different e-Business transaction modes, including Business-to-Business, Business-to-Customers and Business-to-Government.

Despite the fact that this diffusion is still in its early stages, different parties are showing their interest. For instance, in the banking sector, the majority of local banks have launched online banking services which allow their customers to manage their accounts and pay some utilities bills over the internet. Moreover, local technology providers became more interested in developing and providing e-Business-enabling technologies and services, including customised e-Business applications, e-payment systems and web hosting services. Other e-Business activities, including online retail and delivery services, are also notable. On the government side, two actions characterise its interest in e-Business[1]. First, it enacted The Electronic Transaction Law, which was introduced to be applicable to any transactions that may include electronic processing, transmitting and storing of data (ETL, 2001). The law attempts to regulate a number of e-Business aspects including electronic contracts, recodes, messages and signature. It seems that this step came as a response to a number of economical changes and international agreements signed by Jordan. According to Obaidat (2001), after the government had liberated the economy and entered into a number of international agreements, including Jordanian-European Partnership Agreement, World Trade Organisation (WTO) membership and Free Trade Agreement with the Unites States, the economic environment became ready for e-Business activities, therefore, regulating the online environment was an important step to be accomplished by the government. The second notable government step was introducing the national e-

[1] Government literature uses the term e-Commerce which is included in this study's definition for e-Business.

Commerce strategy in 2008 which reflects its desire to exploit the potential benefits of e-Business at a national level (MoICT, 2008). This strategy came as a reaction to the government policy for ICT and postal sectors which called for more efforts to encourage local companies to offer e-services, especially e-Commerce services (ICT-Policy, 2007). The strategy action plan attempted to cover a wide range of e-Business areas including technology, laws and regulations, transportation and logistics, utilities, customs, taxation and financial services.

Nevertheless, security aspects of the e-Business environment in Jordan are not getting very much attention. Several security issues are frequently reported by international organisations as well as a few interested researchers. For instance, a security assessment performed by McConnell International (2002) highlighted the need for improvement in several areas of information security. Its report identified issues such as the lack of cyber crime and privacy laws, digital signatures and e-payment infrastructure. The report emphasised the importance of establishing a secure e-Business environment by enacting cyber crime law, secure transaction certificates and privacy laws. Also, it highlighted the need for developing an infrastructure that enables secure e-Business, and it recommended the development of encryption infrastructure. Other unsettling results in a United Nation's report ranked Jordan at maturity level one, which is "characterised by an almost total absence of data security, privacy policies and laws governing ICT abuse" (ESCWA, 2007).

Although little academic research can be found in relation to this problem situation, it gives us an indication that security issues exist in the context of the study and represent a serious barrier for e-Business adoption in the country. For instance, a survey of 453 Jordanian consumers (Alsmadi, 2002) found that while those customers are likely to have enough knowledge and skills to use the internet, online security is a major factor that prevents them from online shopping. Similar findings were reported by a recent survey (Khasawneh, et al., 2009) covering a random sample of 270 internet users from Jordan.

While these surveys bring the customer side of the problem to the forefront, other studies shed light on the security concerns of organisations willing to adopt e-Business. Titi (2005) surveyed 110 Jordanian business managers and asked them to select from a list of potential barriers that could limit the adoption and emergence of e-Business in Jordan. The list included security in addition to other barriers such as skills and expertise, customer

readiness and cost. Two-thirds of the sample stated that privacy and data security are among the major barriers. Another related barrier highlighted by the survey was the difficulty that companies face when dealing with legal issues such as electronic signatures and contracts, as well as consumer rights. A more recent study has used a case study to identify factors influencing e-commerce adoption in a private company in Jordan (Al-Qirim 2007). It reported the company's concerns about the lack of confidentiality of information processed by e-commerce systems in addition to the lack of secure local infrastructure, including secure e-payment systems and an effective legal framework to regulate online activities. The case study found that these issues complicate the process of adoption and securing e-Business as companies would be required to get in touch with international service providers which involves extra time, effort and cost. In an attempt to explore e-commerce security perception of customers and organisations as a single phenomenon in the context of the study, Halaweh and Fidler (2008) found contradictions between customers and business perspectives in how security concerns are better addressed. The study has revealed that online companies give more weight to tangible security features to encourage customers to use their websites; they use trusted third party logs, privacy policies or statements to the customers telling them that the website is secure. On the other hand, customers were found to be less interested and less aware of such features; they looked for intangible features such as company identity, brand name, and reputation.

While these previous studies raise our attention regarding e-Business security in the context of Jordan, they do not offer a deep analysis of the problem situation; this in turn limits our understanding of the various aspects that need to be considered to develop a secure e-Business environment. The limitations emerge from the fact that most of these studies did not consider security as their primary focus; therefore, little effort has been devoted to exploring this issue in detail. Moreover, the positivist approach underlying most of these studies limited their findings into a set of specific questions which often try to explore the existence of predefined security issues without offering an explanation of how and why these issues emerged. Even when other studies have attempted to explore the problem domain using an interpretive approach which can give more insight into e-Business security, only one or two stakeholders (customer, business or both) have been considered, which did not help in addressing the influence and requirements of other relevant stakeholders such as government and technology providers. To this extent it can be argued

that the existing literature does not capture the complexity of the problem domain nor develop knowledge and/or understanding of the various associated issues. This encourages the researcher to develop better research design to fill the existing research gap. By combining the socio-technical perspective and stakeholder analysis with a well-designed knowledge generating approach, a holistic understanding of e-Business security in the context of the study is likely to be developed. Such understanding can be extended to generate ideas to deal with the multifaceted nature of the e-Business security problem.

1.2 Aim and Objectives

In the light of the above identified research gap, the overall aim of this research is to develop a conceptual framework for better understanding of the problem of e-Business security based on an interpretive stakeholder inquiry. This aim will be achieved through the following objectives:

1. To identify the multifaceted nature of information security within the complex and dynamic e-Business environment.
2. To construct a framework of inquiry to allow the researcher to investigate the e-Business security environment from a socio-technical perspective.
3. To identify the various groups of stakeholders involved in the context of the study and explore their interrelationships and roles toward e-Business security.
4. To identify the set of socio-technical factors affecting the e-Business security environment and their interrelationships.

To fulfil these objectives the following general research question is formalised:

> How can security be incorporated in e-Business in the context of the study to provide a trustworthy e-Business environment which considers the roles and requirements of the various security stakeholders?

To answer this question four specific research questions representing the units of analysis in this research are formalised:

1. How is security of e-Business approached by technology providers in the context of the study? And what are the implications of their interactions with other stakeholders?

2. How is security of e-Business perceived and addressed in e-Business organisations in the context study?
3. How do customers' perceptions, awareness, education and expectations affect e-Business security in the problem situation?
4. What is the current role of the government regarding e-Business security? And how it can be an effective partner in the problem situation?

1.3 Summary of Contribution

This thesis is expected to contribute to the growing body of research in the field of information security in general and e-Business security in particular for the following reasons:

1. The literature review shows that few stakeholders are likely to be considered, predominantly, customers and internal organisations, and this significantly limits our understanding of the role and the effect of other important stakeholders such as governments and technology providers. In contrast, this study uses the concept of "e-Business stakeholder" as a meta-theory to facilitate deeper understanding of security in the e-Business environment. Consequently, an interpretive stakeholder analysis was used and four major stakeholders in the problem situation were identified and their security implications were explored. These stakeholders included: technology providers, e-Business organisations, government and customers.
2. Through an inductive coding process an explanatory framework of organisational, legal, human and technical factors affecting security in e-Business environment has been developed. Additionally, the study brings these factors together, identifies their interrelationships and implications, and positions them in the relevant existing knowledge.
3. While the literature calls for more socio-technical information security thinking, this study contributes to this emerging body of research with empirically grounded security research adopting the socio-technical perspective as an underlying assumption for its inquiry which will help in identifying and better understanding the various dimensions affecting e-Business security environments.
4. The study also contributes by developing a complete research design which shows how the case study method as a research strategy can be combined with the general

inductive approach realised through thematic framework analysis to provide a systematic and rigorous methodology.

The study theoretical, methodological and practical contributions are discussed in more details in Chapter 8, Section 8.2.

1.4 Structure and Contents

This section provides an overview of the contents of this thesis. Figure 1.1 illustrates its structure which consists of eight chapters.

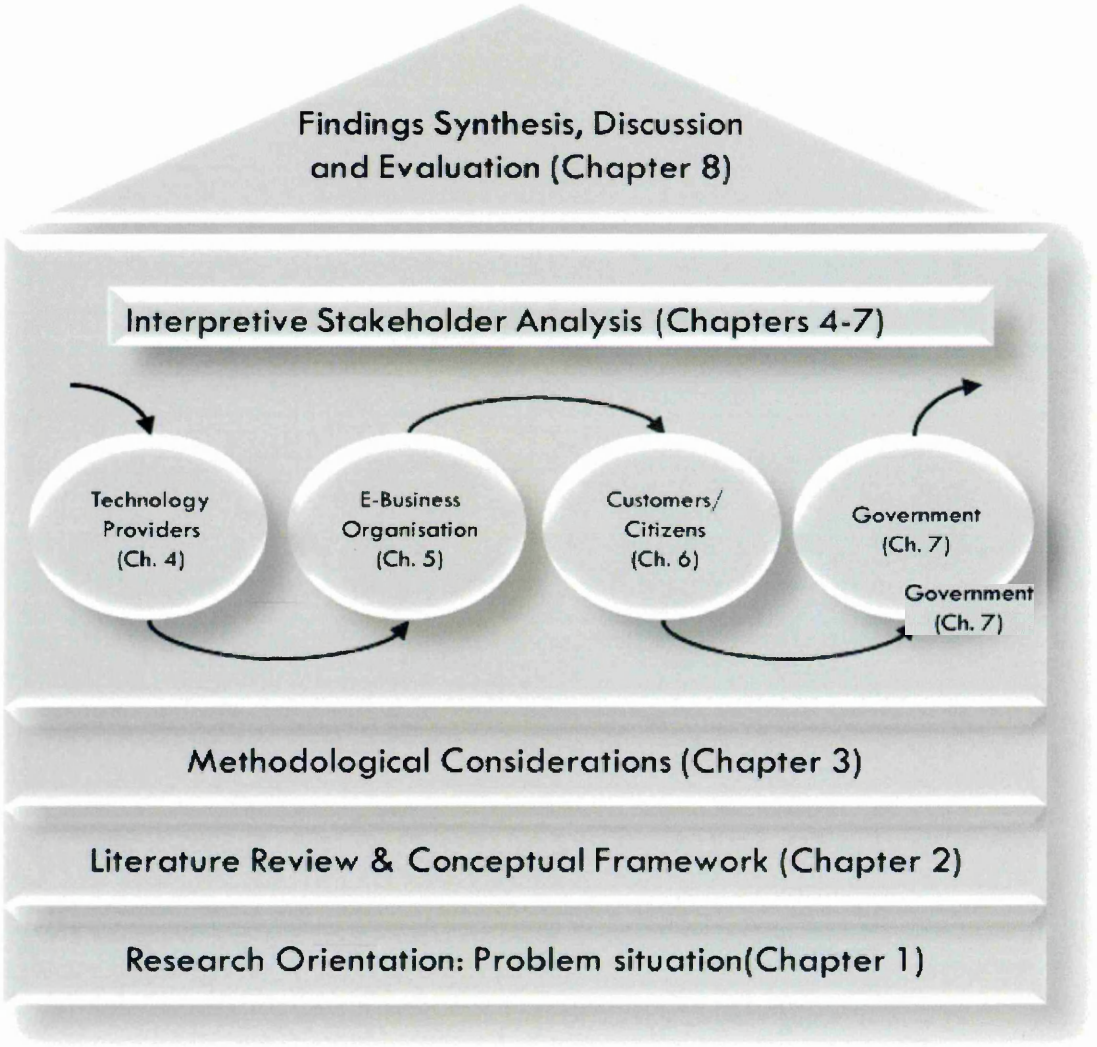

Figure 1.1: Structure of the Thesis

The first three chapters of this thesis set out the theoretical and methodological foundations of this research. **Chapter 1** sets the scope of this research which is concerned with e-Business security and describes the research context. Additionally, it defines the study's aim and objectives and formulates specific research questions to be answered by this study. Towards the end, it briefly summarises the expected contributions of the study. **Chapter 2** reviews the literature and builds a conceptual framework to guide inquiry of this research. It sets the study's terminology by defining and discussing the basic terms, concepts and issues associated with e-Business and information security. Moreover, it presents the current trends in information security research, including e-Business security research, and critically evaluates the major research contributions which represent a paradigm shift in this domain. **Chapter 3** discusses the methodological considerations in the process of selecting a suitable research method for conducting the inquiry. After identifying the research assumptions underlying each available research method and assessing their potential for this study, a justification of the selected research method is given; this followed by a complete research design including research strategy, data collection techniques and analysis procedure.

Through an iterative and inductive coding process, four major security stakeholders in the context of the study have been identified and their security roles have been explored. These stakeholders are technology providers, e-Business organisations, customers/citizens and government. Analysis and findings of these four units of analysis are presented in **Chapters 4-7**.

Finally, **Chapter 8** synthesises the four units of analysis and discusses their findings. It brings together the main findings and identifies their interrelationships and implications. Additionally, it discusses the thesis's theoretical, methodological and practical contributions, as well as providing an evaluation for the overall research process and ends with possible future research directions.

Chapter 2 : Literature Review and Conceptual Formwork

The proliferation of Internet technologies has encouraged organisations to reshape their business models to achieve several advantages such as increasing their productivity, profits and customer satisfaction. This increases the flow of electronic information, either between businesses or between business and customers, which raises many concerns about the secure storage, processing and exchange of this information. Consequently, the term 'information security' has evolved to include other issues with a strong social foundation such as trust, privacy, legal liability and intellectual property rights (Beznosov & Beznosova; 2007). Additionally, several parties became involved and have interest in this domain; these include governments, citizens/customers, and businesses along with technology vendors and academic researchers (Chu et al., 2005).

Unfortunately, a great deal of research work in security has focused on producing theoretical models or technical solutions without addressing the real world where the research outcomes are supposed to be used (Siponen & Oinas-Kukkonen, 2007; Clarke, 2001). This gives a clear indication that there is a lack of understanding of the security problem as well as the effect of its context.

This chapter reviews the relevant literature and defines the key terminology in order to establish a conceptual foundation to support the research inquiry identified in the previous chapter. It discusses how traditional security approaches and pure technological solutions are not sufficient to provide adequate security for today's complex electronic business environment. It also identifies the trend in information security research and highlights the need for new approaches for e-Business security. Additionally, it reviews and compares the major research contributions which represent a shift and a new paradigm in the field of information security. Finally, it presents a conceptual framework of inquiry to guide this research.

As this study is inductive and seeks to generate knowledge rather than to prove or test a theory, the role of literature in such an interpretive qualitative study is worth clarifying. In

contrast to theory-testing research, which depends on conducting a comprehensive review of pre-existing theories and literature prior to the data collection phase, the literature review in inductive research is a continuous process throughout the whole research. At the beginning of the research it serves as a foundation for the study's conceptual framework which identifies the boundaries of the study including the main aspects to be investigated (Miles and Huberman, 1994). This framework should not be based on an overly comprehensive review as this will constrain the exploratory power of the study (Josselson and Lieblich, 2003 in Rudestam and Newton, 2007). Therefore, the initial review should be to an extent which informs the reader about the existence of the problem and why it is worthwhile. Creswell (2007) suggested that the qualitative researcher should review the literature to build a rationale for the problem and place his/her study within the ongoing literature about the topic. The initial review is also important for demonstrating the underlying assumptions and the theoretical perspective behind the general research questions (Marshall and Rossman, 1999). Additionally, it defines the topic's key terminologies that will be used throughout the study. The content of this chapter reflects the roles for the literature review discussed above. As the study evolves and moves into the data collection and analysis phases the literature can be used to develop explanations, validate findings and suggest interrelationships between them (Richie et al., 2003; Marshall & Rossman, 1999). Towards the end of the study the literature plays an important role in discussing the emerged findings, positioning them within existing knowledge and seeking wider implications (Rudestam and Newton, 2007).

2.1 e-Business overview

This section provides an overview of e-Business as an emergent concept; it starts by reviewing and critically evaluating the existing definitions in an attempt to formulate a working definition of e-Business to be used by this study, then it discusses e-Business components and transaction modes, highlighting the complexity of its environment. The overview also discusses the potential benefits of e-Business followed by the associated adoption issues with more emphasis on the security issue which is then discussed in more detail in a separate section.

2.1.1 A working definition for e-Business

In its broad sense electronic business, or simply "e-Business", refers to the use of Information and Communication Technology (ICT) for various business activities. One of the early definitions of e-Business is provided by IBM which defines e-Business as "*a business process transformed to leverage WWW (Internet, intranet, and extranet) technology for business benefit. It is about using the Internet infrastructure and related technologies to enable business anywhere and anytime*" (Smith, et al., 2001). However, the definition may differ from one perspective to another, which usually causes confusion with other terms such as e-service, e-commerce and e-learning. Often the term e-Business is confused with e-Commerce (Turban et al., 2008), and this should be clarified before choosing a working definition for e-Business in the context of this study.

When compared to e-Commerce, e-Commerce is regarded a sub-set of e-Business, which is much broader and may include most business activities (Groucutt and Griseri, 2006). E-commerce is used to describe online buying and selling activities, which can be viewed as a contact-driven process (Rodgers, et al., 2002) which requires the customer to get in touch with an online company in order to initiate the process. On the other hand, many e-Business activities might be accomplished without human intervention. E-Business is an umbrella term for a wide range of business processes which may include one or more of the following: customer relationship management; enterprise resources planning; and supply chain management.

Many valid e-Business definitions can be found in the literature (de Graaf and Muurling, 2003). For example, Clarke (2000) defines it as "*the conduct of business with the assistance of telecommunications and telecommunications-based tools*". Clarke's definition does not specify any specific communication technology for conducing e-Business, which makes it applicable to the wireless and mobile technologies which are utilised these days in e-Business. Nevertheless, if we consider the communication media and related tools as infrastructure for the Internet, IBM's definition encompasses Clarke's definition as well. Tracy (2000) argues that the definition of e-Business varies; however, it is usually similar to IBM's definition.

A preliminary investigation of the study environment revealed that the majority of e-Business adopters have a partial e-Business transformation in the shape of e-Commerce

activities such as online order, e-payment, online customer service and e-billing. If IBM's definition, which implies a complete transformation of business processes using Internet technology, is adopted, few companies from the study context will fall under this condition. Business to customer interaction is viewed as a partial transformation of business processes and the complete transformation involves company to company interaction (Tracy, 2000). Therefore, the study will consider both the partial and complete transformation of business process using Internet technologies as the basic definition for e-Business in this study. Many e-Business startups do not use e-Business to its full potential. We could find some of them using ICTs to improve their internal business operations. Others may use the web service for marketing purpose or for price comparison. Those who have just started simple e-Business initiatives or just use ICTs to improve their business, will after few years be forced to upgrade their simple models of e-Business to include ordering, payment, contracting, invoicing and delivery. For this purpose we may define e-Business in a broad way to include any utilisation of ICTs in these organisations to help them improve business and interaction with government, customers or suppliers.

2.1.2 e-Business components and transaction modes

E-Business transactions include two or more parties such as customers, sellers, suppliers, intermediaries or business partners: see Figure 2.1, which views e-Business as a process that spans the entire spectrum of human activity (Cunningham and Froschl, 1999). Although this framework abstracts the complexity of the e-Business environment, it identifies three main e-Business components; *enabling technologies* (Internet or Intranet), *stakeholders* (customers, suppliers, regulators and financial institutions) and *business processes* (internal, intra-organisational and with customers). This implies that e-Business can be viewed as a socio-technical system with a set of interacting elements. Some of these interactions may involve direct intervention from a particular stakeholder; for example, a customer placing an online order through the seller website. Other interactions may be performed without intervention and on behalf of the interested stakeholders; for example, credit card information is checked automatically on behalf of the merchant. Based on the nature of the transaction and the relationship between the transacting parties, e-Business can be classified into different modes (Turban et al. 2008). Accordingly several e-Business modes can be found:

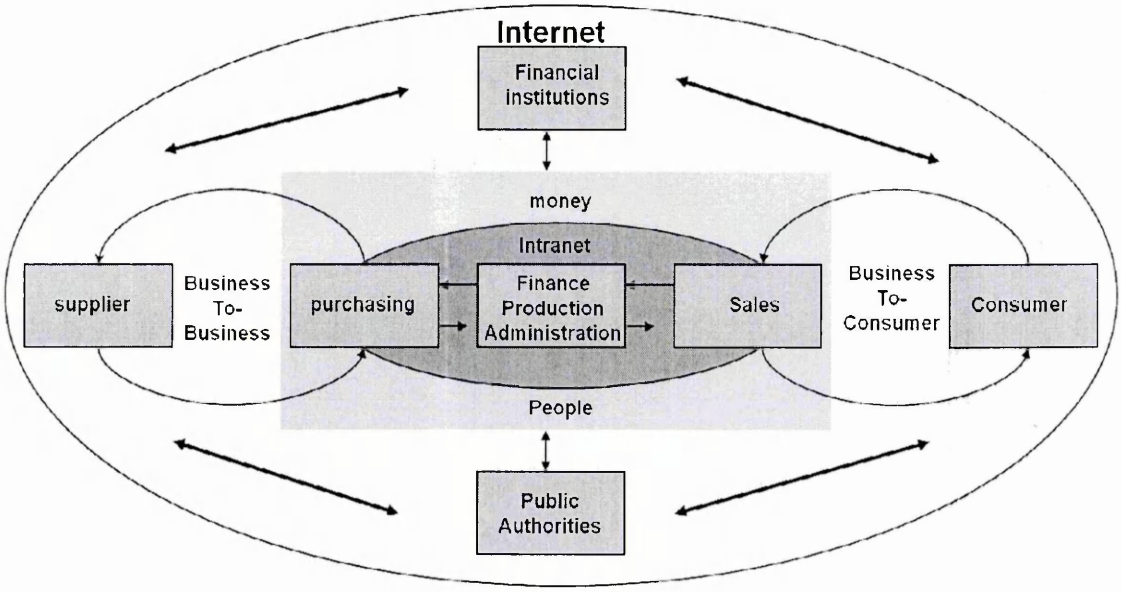

Figure 2.1: The Electronic Business framework (Cunningham and Froschl, 1999).

- ***Business-To-Customer (B2C)*:** Electronic commercial transactions directly between business (mainly private organisations or companies) and individual customers. Many examples of companies using B2C mode can be found worldwide. A good example is the well-known online bookshop Amazon.com. Amazon.com started with selling books online: a customer can go to its website, select the book s/he wants, pay online and then the book will be delivered to customer's address. Nowadays, Amazon.com is not only an online bookshop; it sells many other items. Another example of a well-known B2C company is Dell Computers. This is one of the first companies which realised how the B2C mode could improve its business and increase its customer satisfaction. Through the Dell portal, the customer can place an order, check the status of his order, get technical support and access many other services.

- ***Business-To-Business (B2B)*:** This mode includes different business processes and activities between business partners (usually private organisations). This mode can be further classified into inter-organisational and Intra-organisational e-Business. The first type represents the internal business process automation in which many internal business activities such as production, invoicing, inventory and accounting

have been integrated and automated through the use of Enterprise Resources Planning systems (ERP). The second type includes Intra-organisational activities with suppliers and distributors which have been automated using e-Business technologies. An example of an application using this mode is the Supply Chain Management systems (SCM).

- ***Customer-To-Customer (C2C)***: In this mode, customers can directly sell and buy from each other over the internet. A good example of the C2C e-business mode is ebay.com which is an online marketplace where sellers and buyers can meet and communicate in order to sell or buy new or used items. It is an online platform for direct trading between customers.

- ***Business-To-Government (B2G)***: Provides information regarding contracts and business investment that the private organisations want to do with the government. This mode can be considered as a bidirectional mode, either G→B or B→G. Some governments provide a central online portal for private business owners and suppliers who want to sell services or goods to governments. Such government websites may contain all the relevant information about government tenders, announcements, or requests for proposal. In the other direction, some private organisations provide information about services that the government can get from them through websites containing product description, promotions, offers and other information customised to suit the government's needs.

- ***Government-To-Citizen (G2C)***: Provides citizens with access to a government information service or/and electronic transactions such as e-Voting, e-Tax. For example the Jordan e-Government portal (http://www.jordan.gov.jo) provides a central government portal where citizens can search for and find information and services provided by the Jordanian government.

B2B represents the largest percentage of e-Business transactions worldwide (Mockler et al., 2006). On the other hand, B2C is the second largest and earliest form of e-Business. Following the argument for selecting a broad definition for e-Business, this study will focus on B2C in addition to B2B for the following reasons:

- B2C mode is the predominant e-Business mode in the study environment.
- It is a feasible option for small private companies in developing countries, bearing in mind that these companies count for more than 70% of all employment in developing countries (Payne, 2002).
- B2C affects a wider range of stakeholders; individual consumers, businesses from small to large, technology vendors, and governments which are responsible for protecting their citizens. Thus, many implications need to be considered.

2.1.3 Potential benefits of e-Business

Numerous e-Business benefits are reported in the literature (Kalakota and Robinson, 2001; Rodgers et al., 2002; Amor, 2000; Smith, et al. 2001; Sanders, 2007; Turban et al., 2008). As many of these reported benefits are a result of real world case studies and surveys, they reflect the positive impact of the adoption of e-Business on different levels of society. E-Business creates new relationships between businesses and customers which can be personalised to suit different customers' needs, and hence increase customers' satisfaction. Also, it enables more efficient co-operation between business partners. Smith, et al. (2001) argue that e-Business could lead to higher customer satisfaction for numerous reasons, examples of which are that customers have personalised 24x7 access to online business and that information is better, faster, and easier to access. Another benefit to companies is increasing company visibility (Amor, 2000) which is very important for newly established ones. Because of the availability of the internet, this can be achieved at a lower cost and can lead to increase in company revenue. Moreover, internal business process automation and intra-organisational interaction facilitated by e-Business technologies is likely to improve company performance and enhance communication (Sanders, 2007). Following the classification of Turban et al. (2008), these benefits can be summarised as shown in Table 2.1.

Table 2.1: Summary of e-Business benefits.

Classification	Potential Benefits
Benefits to Organisations	– Reducing cost. – Improving Performance – Expanding to new markets – Improving communication with partners and customers – Improving availability and accessibility – Increasing visibility
Benefits to Customers	– Lower Prices – More choices – Less physical effort – Personalised products and services – Information availability
Benefits to society	– Increasing Business opportunity – Reducing traffic and pollution (people work or shop from home) – Greener world and less paperwork – Better standard of living

In contrast to the above very optimistic view about the potential of e-Business, other researchers seem more realistic. For instance, Siddiqi et al. (2002) argue that many of these claimed benefits cannot be guaranteed because of several cultural, technological and economical barriers to the growth of e-Business. They discuss a number of B2C scenarios in which potential benefits such as convenience, cost-effectiveness and capability requirements cannot be realised for many reasons such as the nature of products, usability issues, hidden costs and user socio-technical requirements. Despite the fact the e-Business seems promising and has many potential benefits, the adoption process is not straightforward and there are diverse issues hindering the proliferation of e-Business. The next section will discuss these impediments that need to be considered if the adoption of e-Business is to be fruitful.

2.1.4 e-Business adoption issues

The adoption of e-Business has an impact on organisations; it improves efficiency and productivity, opens new market channels and increases the competitive position of the organisation. On the other hand, it has several impediments and raises many issues. The rapid development of e-Business introduces serious issues regarding privacy, information

security and other legal, ethical, and social issues (Li, 2007). Many researchers have discussed e-Business issues in terms of inhibitors, impediments and barriers (Papazoglou and Ribbers, 2006; Baršauskas and Sarapovas, 2004; Jennex and Amoroso, 2002). In general we may categorise these issues as:

- *Technological Issues*: implementing and deploying e-Business initiatives requires knowledge and skills related to various Internet technologies and infrastructure which are the building blocks for e-Business. Several studies suggest that the lack of in-house technical skills prevents companies from implementing and running e-Business systems (Chapman et al. 2000; Windrum and Berranger 2004). Other technical issues are related to interoperability and compatibility of legacy systems with new ones. Deploying e-Business applications such as CRM, ERP, and SCM involves consolidating data from different sources which usually reside in legacy systems; this requires integration and business process reengineering to enable these systems to work together. Most of the time, this integration is not an easy task because the legacy systems were built based on standards which do not support Web services supporting e-Business applications (Chen, 2003).

- *Financial Issues*: in many countries the cost of setting up online business is still high. The cost includes Internet connection, web hosting, delivery costs, staff training and the cost of hiring skilful employees. Such financial issues are more notable in small companies (Al-Qirim, 2004). However, costs have started to decrease and more companies and customers have begun to benefits from the new technology.

- *Trust, Privacy and Security Issues*: according to many studies the lack of adequate mechanisms to protect sensitive information about customers, such as credit card information, makes people reluctant to engage in e-Business transactions (Udo, 2001; Kim et al., 2009). Moreover, the use of data mining tools to collect customers' information increases concerns about privacy in customers who do not want to lose control over their personal information (Scott, 2004). These concerns contribute to the issue of trust on the Internet which represents a challenge for many companies, since people used to trust merchants whom they knew face-to-face and this is not the case on the internet (McCole et al., 2009).

- *Legal and Regulation Issues*: in many countries there is still no clear legal framework for e-Business (ESCWA, 2007). Issues related to intellectual property, liability and taxation need to be considered (Frynas, 2002). Other issues are related to the legal recognition of electronic records and some security mechanisms, such as digital signatures, as legal evidence in case of dispute resolution.

- *Management and Cultural Issues*: the lack of clear vision and strategy for how a company may benefit from e-Business initiatives and in some cases the lack of management support make a barrier for successful e-Business adoption (Dezalak, et al., 2006). Other issues are related to changing business processes and how people react to such changes. Employees might resist using new technology in their work, and here good management is necessary to help staff accept and use new technologies (Somers and Nelson, 2004).

In addition to the above issues, developing countries have other issues that are worth mentioning. The use of e-Business in the developing world which represents a large part of the marketplace is still insufficient. The use and development of e-Businesses in this part of the world is faced with many challenges and issues. Without serious effort to remove these challenges, developing countries might not benefit from the great technological revolution. Deployment of ICT, which is the backbone of e-Business in developing countries, is facing many obstacles and constraints. These include lack of or poor infrastructure, social problems and the lack of an appropriate legal, political and economic framework (Bakari, 2007; Jennex and Amoroso, 2002). Some e-Business barriers which particularly face developing countries are (Gregorio D. at al, 2005; Kshetri, 2007):

- Low levels of Internet and personal computer penetration.
- Poor e-Business infrastructure including ICT, logistics and fulfilment.
- Low level of credit or debt card penetration.
- Lack of e-payment gateways.
- Computer illiteracy in general, lack of knowledge about e-Business and lack of basic English language skills.
- Preference of traditional face-to-face communication over other means such as e-mail and instant messages.

Dada (2006) argues that effective e-Business depends on a critical threshold of online use. This suggests that, as more people use the Internet, the network value and the opportunity for e-Business will increase. Unfortunately, the online population in developing countries is far from the critical threshold. According to Pahladsingh (2006) there are a number of barriers to increasing the online population in these countries; they are: low level of computer penetration, because of the high cost of having a personal computer; the cost of Internet connection (using technologies such as Dialup or Broadband); unreliable communication infrastructures; cultural issues such as the language barrier; and other economic, political and business issues.

In the context of Arab countries, including Jordan, similar adoption barriers have been reported by recent studies (Pons et al., 2003; Yasin and Yavas, 2007; Al-Qirim, 2007; ESCWA, 2007). Remarkably, security of e-Business is frequently citied as one of the major issues that impede both consumers and business organisations from utilising e-Business in these countries. Yet no previous study has attempted to explore this issue in detail and in relation to other adoption barriers and stakeholders. E-Business security issues will be the primary focus of this study, but in contrast to the previous studies, which considered security from a very narrow perspective and in isolation from its wider context, this study will consider the multifaceted nature of e-Business security in relation to its context and stakeholders. As a starting point for developing a framework of inquiry to guide this study, the next section discusses the concept of the "e-Business stakeholder" as a meta-theory to facilitate deeper understanding of security in the e-Business environment.

2.2 Stakeholder analysis and its potential for exploring e-Business

Doing business online makes organisations potentially more vulnerable than in any previous time. In the e-Business era, such organisations have more channels for exchanging information and services with several interested parties within the electronic environment, including customers, suppliers and business partners. They are able to reach more customers in different geographical areas, subject to several national and international legislations governing various e-Business activities and constrained by social, ethical as well as technical factors. Consequently, the business environment has become wider than any time before and more factors from outside the organisation's influence may determine the way an organisation works. In such a situation the level of uncertainty about this

environment increases, leaving the organisation subject to additional risks especially with different and conflicting stakeholders' interests. This suggests that e-Business cannot be studied in isolation from its environment and wider implications need to be considered. As a starting point for exploring this complex and dynamic environment it is important to identify all the interested parties and investigate their interrelationships, interactions and impact on the e-Business environment. This can be achieved by the use of stakeholder analysis which facilitates holistic understanding of the problem situation.

It has been argued that stakeholder analysis is not so much a unique research approach but is an organising principle for research which can be used within various research methods (Burgoyne, 1994). It captures the diversity of perspectives and interests in the problem domain, allowing the research to develop a richer picture which facilitates better understanding of the problem in hand. The foundation of stakeholder analysis is the concept of the "Stakeholder". According to the stakeholder theory (Freeman, 1984; Donaldson and Preston, 1995) an organisation is surrounded by a set of stakeholders. A Stakeholder is any individual (such as a customer), or organisation (such as business partners) influenced by the attainment of the organisation's goals, and who is likely to hinder this organisation's achievement if its own requirements are not fulfilled. Stakeholder can be defined by two functions (Philips et al., 2003); a utility function that measures the level of the stakeholder's satisfaction, and an influence function that measures the damage or benefit the stakeholder can cause an organisation given a level of utility. According to Philips et al., the organisation should work towards minimizing the damage and maximizing the benefit. Freeman (1984) provided a general definition for the term "*stakeholder*":

> "A stakeholder in an organization is (by definition) any group or individual who can affect or is affected by the achievement of the organization's objectives" (Freeman, 1984, p. 46).

The definition highlights different aspects that need to be considered when using the stakeholder concept:

1. A stakeholder can be either a group or an individual.
2. The relationship between the stakeholder and the organisation is bidirectional.
3. The impact/influence is either negative or positive.
4. The stakeholder's interest versus the organisation's objectives.

Although the notion of the stakeholder has its roots in management literature, it has been used extensively in Information System (IS) studies (Flak and Rose, 2005; Papazafeiropoulou et al., 2001; Avison and Wood-Harper, 1990; Pouloudi and Whitley 1997). Pouloudi (1999) has reviewed extensively the use of the stakeholder concept in IS literature. Based on that, she argued that stakeholder analysis is implicitly embedded in IS development approaches such as Soft System Methodology (SSM) and Effective Technical and Human Implementation of Computer-based Systems (ETHICS) method which both emphasise the involvement of all interested parties in the IS development process. She concluded that:

> The notion of stakeholder is not new in information systems research. Although the actual use of the term is relatively recent it does not signify a revolution or 'paradigm shift' in our thinking of information systems development and implementation. It represents a progression from developer- and user- centered problems to organization-wide and interorganizational information systems problems. It is also a sign of maturity of Information systems research as it reflects a shift towards approaches that can afford a more holistic representation of the parties involved in the more complex systems currently developed. (Poulodi, 1999, p. 14).

In the realm of information security a number of authors use the stakeholder notion in order to get more insight into the socio-technical aspects of security problems, but without explicitly acknowledging the use of stakeholder analysis. For instance, Flechais and Sasse (2007) used "participant" analysis to investigate usability issues of security mechanisms by exploring how participants perceive and interact with security. They did not use the terms stakeholder analysis, however the concept of stakeholder was the primary component of their final model. Other researchers use the same approach to investigate how the commitment of different stakeholders affects security awareness training in organisations (Abawajy, et al. 2008). On the other hand, explicit references can be found in quite similar fields; for instance, Shankar et al. (2002) used the stakeholder theory to propose a theory which incorporates a multi-stakeholder perspective for trust in the online environment.

Arguably, this theory is much needed in order for today's e-Business organisations to survive in the complex environment of e-Business. Donaldson & Preston (1995) identify three aspects for stakeholder theory; *descriptive, instrumental* and *normative* aspects. The researcher suggests that these aspects are helpful and can be applied in this domain. The descriptive aspect of the stakeholder theory can be used describe the e-Business

environment and identify its stakeholders, however, its instrumental aspect can be used to explore the linkages or lack of linkages between the e-Business stakeholders. This implicitly implies looking for the implications of their interrelationship and interaction with the e-Business environment, hence the use of impact analysis. The normative aspect of the theory can be used to explain the security role of each stakeholder from an ethical point of view. Both descriptive and instrumental aspects of the stakeholder theory will be used in the study to facilitate a deeper understanding of problem situation.

2.3 Toward a Stakeholder Model for e-Business

Different type of stakeholders may be involved in e-Business transactions. Using the e-Business concept model (see figure 2.2) proposed by Jones et al. (2000), e-Business transaction can be viewed as a set of interacting components including stakeholders, information and infrastructure:

1. Stakeholder: a person or organisation who is, or is likely to be, significantly affected by e-Business. The three categories of stakeholder are: **participating** (*those who are doing business by means of using e-business services and technologies*), **enabling** (*those who provide services or technologies to enable e-business to take place.*), and **supervisory** (*those who regulate or provide advice on e-business in some way*).

2. Information: such as customer details, company strategy and payment information.

3. Infrastructure: such as public communication networks, intranet, extranet, database servers and payment systems.

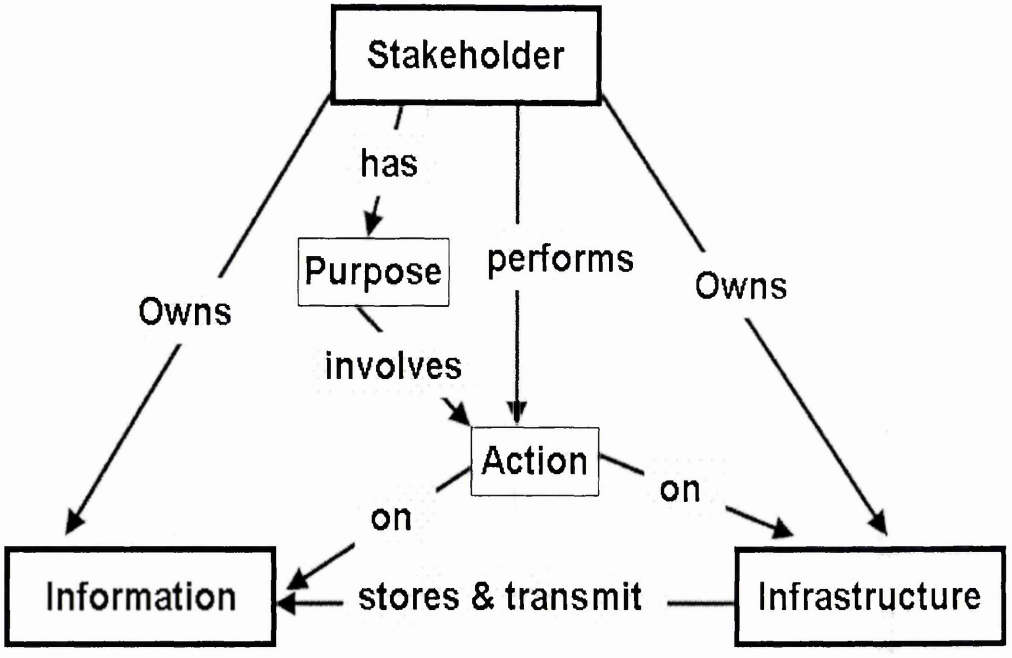

Figure 2.2: e-Business Concept model (Jones et al., 2000)

This concept model tries to conceptualise and identify the important elements of e-Business systems and their relationships in order to abstract the complexity of the problem of e-Business requirements. It is a powerful thinking tool that allows us to view the whole picture instead of having one perspective that may lead to poor specification of requirements. The model clearly acknowledges that the concept of e-Business cannot be viewed without the concept of the stakeholder, which represents an entity owning information and infrastructure and having a particular purpose and interrelationship with other entities in the e-Business environment

A recent evaluation of e-Business research (Chua et al., 2005) revealed that, unfortunately, researchers are likely to focus on only a few stakeholders, predominantly, customers and internal organisation. The study also points out that other stakeholders such as regulators, suppliers, investors and indirect stakeholders require more attention for the following reasons:

- E-Business cannot be fully understood if important constituents are ignored.

- The interdisciplinary nature of this field forces the researcher to understand how the stakeholders interact.

- The need for revealing emerging issues related to this field.

In this study stakeholder analysis will be used as an overall organising principle to create a richer picture for the e-Business environment as an attempt to consider the role of other important stakeholders along with customers and e-Business organisation. Government, citizens/customers, private sector e-Business organisations, business partners and technology providers are key players in the e-Business game. They have different roles and goals; however, together they play an important role for successful e-Business in a particular country. In exploring e-Business security from a holistic perspective, this study will focus on four stakeholders who represent the primary interested parties who may benefit from, be influenced by, or affect, e-Business security in the context of the study; a conceptual stakeholder model showing those different parties is shown in Figure 2.3.

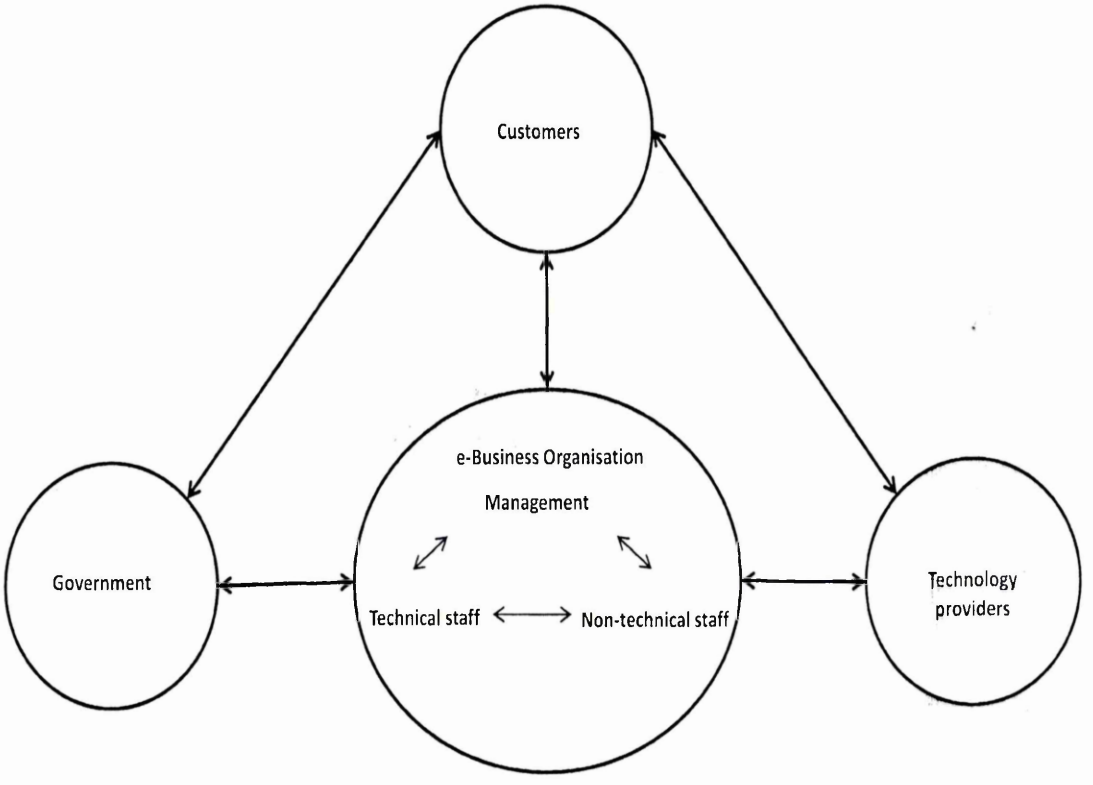

Figure 2.3: Study e-Business Stakeholder Model

Each of the stakeholders has its own perspectives, requirements, and interactions with the others; if these are studied in isolation, many security aspects will be overlooked. Some of the stakeholders may control the environment; for example, the government regulates e-Business activities and enforces the various laws controlling e-Business in the country. However, the others may have a great influence on e-Business environments, such as the technology providers who provide the required infrastructure for deploying e-Business. Therefore, a bidirectional relationship should be considered between the stakeholders. Arguably, exploring the roles of those stakeholders, their perspectives and interactions, will generate a better insight into how security can be incorporated in the e-Business environment.

To explore the security role of each of those stakeholders, they will be incorporated in a conceptual framework guiding this study in the different dimensions influencing security in e-Business environments. Before building this framework of enquiry an overview of e-Business security will be given.

2.4 e-Business Security Overview

Security in its broad meaning plays a major role in successful e-Business adoption. Without having security in place, e-Business transactions cannot be realised, as security is the only way to verify the identities of the transacting parties and prevent any potential risks which could harm them or their information. Research findings show that many customers and business owners are reluctant to engage in any online business transaction because of security concerns (Udo, 2001; Kim et al., 2009). There is a gap between the predicted volume of online retails and the actual development; one of the major reasons for this gap, backed by many studies, is the lack of trust, privacy and security in digital business (Katsikas et al., 2005; Scott, 2004).

As this study is concerned with the security of the e-Business environment it is important that the concept of security and issues related to this topic be clarified. In the following sub-sections, definitions of security and information security services required by e-Business systems are discussed.

2.4.1 Security is hard to define

Security is hard to define, since the meaning changes from context to context. One may define security in term of Confidentiality, Integrity and Availability. A secure system is one which ensures these three objectives by providing the necessary mechanisms and procedures to prevent any unauthorised access, modification or interruption of the services or information provided by that system. However, interpretations of these objectives are influenced by different factors and stakeholders which lead to different security perspectives. As Bishop (2003) points out:

> ...Security rests on confidentiality, integrity, and availability. The interpretations of these three aspects vary, as do the contexts in which they arise. The interpretation of an aspect in a given environment is dictated by the needs of the individuals, customs, and laws of the particular organisation (Bishop, 2003).

Still there is a lot of misunderstanding about the concept of security. Many people, especially non-security experts, associate security only with confidentiality of data. This can lead to a fatal misinterpretation which increases the chance that other security requirements will be overlooked (Knorr and Rohring, 2001). Moreover, there is trade-off between these objectives. For instance, military fields usually focus on providing confidentiality more than other services, because the secrecy of information is very important, so needs to be protected during transmission over communication networks. In contrast, e-commerce services focus more on providing integrity and availability services, where the information relating to transactions should be authentic and not tampered with in any way, and the service should be available whenever it is needed (Bishop, 2003, Schneier, 2008).

Pfleeger and Pfleeger (2003) use a similar definition for security, the "attempts to ensure the confidentiality, integrity, and availability of computing systems' components". In criticizing such definitions, Anderson (2003) argues that these commonly used definitions only describe what security does, without providing an intrinsic concept of completeness or precision in these definitions. He believes that these definitions are very broad and do not help us to identify what information security is not as well as what it is. Therefore, he proposes that security is defined as "a well-informed sense of assurance that information risks and controls are in balance" (Anderson, 2003, p. 310). This definition attempts to provide a more precise view for security and highlights the concept of security assurance

which can be achieved through information security risk management. However, it does not view security beyond the technical perspective which limits security to a list of technical controls which need to be deployed to solve a set of predefined risks.

What also creates a sort of contradiction when dealing with the concept of security is that it is both a feeling and a reality (Schneier, 2008); this implies that existence of the feeling or the reality does not assure the other. For instance, an online company could provide the required technical measures to ensure confidentiality, integrity, and availability of its services; nevertheless, it may fail to make its customers feel secure because it does not appropriately communicate its security to the customers. On the other hand, a customer could be subject to a security risk simply because s/he transacts with a malicious website which makes him/her falsely feel secure. As recognition of both sides of security is important for better security decisions, it is also of equal importance that the definition of security emphasises both feeling and reality. Such a definition is provided by Kiountouzis (2004), who defines security as "an organized framework consisting of concepts, beliefs, principles, policies, procedures, techniques, and measures that are required in order to protect the individual system assets as well as the system as a whole against any deliberate or accidental threat". This definition brings out an important aspect that is missing from the previous ones: it highlights the social elements in the security chain. It views security beliefs and perceptions of people as equally important as the technical controls they interact with. Indeed, this is much needed for today's socio-technical business environments. In another study, Tsujii (2004) presented a comprehensive and interdisciplinary definition for information security and emphasised that technology alone, without strong coordination with social systems, is not enough. He defined information security as:

> the dynamic process for establishing an integrated and complete system of social fundamentals designed to form, without infringing freedom broadened by IT (information technology), and with closer linkage and coordination among technologies, administration and management techniques, legal and social systems and information morals in order to make compatible improved usability and efficiency and enhanced security, protected privacy and minimised surveillance, or monitoring, over people (Tsujii, 2004, p.1).

The previous definition may represent the ultimate goal of information security and gives a picture for the ideal e-society that humans are seeking through utilising technologies. However, this might be impossible since we still trade off between security and usability,

and between privacy and protection. Nevertheless, the definition clearly identifies the different dimensions that influence security and it emphasises that these dimensions should be addressed in an interdisciplinary and holistic way.

2.4.2 Information Security Services for e-Business Systems

Instead of defining security itself, information security literature usually starts by defining the basic security services that should be provided by any system in order to fulfill the various security requirements. Different terms used to refer to these are security related concepts; security basic components (Bishop, 2004); security services (Stallings, 1998) or security objectives (Outeye, 2003). In this study these terms will be used interchangeably to refer to the same thing. A discussion of these security services with more emphasis on the e-Business environment is given here:

1. ***Confidentiality***: During e-Business transactions sensitive and private information is being transmitted over insecure channels. Such transmitted data may contain credit card information or business information. Therefore, there is the need for a security service which prevents unauthorised access to this sensitive information. Confidentiality is concealment of information or resources (Bishop, 2004), to prevent unauthorised entities from being able to read messages sent between authorised parties. Confidentiality is achieved by encrypting the contents of the message with various sophisticated encryption techniques. Cryptography can be considered as an access control mechanism which supports confidentiality. It scrambles the content of the message to make it incomprehensible.

2. ***Integrity***: Integrity is related to the accuracy of data in either the transmission or storage devices. It refers to the trustworthiness of the data or resources. Integrity falls into preventing any unauthorised modification of data or resources, and detecting any modification or simply reporting that the data is no longer trustworthy (Bishop, 2004). Data integrity is very important for e-Business transactions because they are conducted over a distance, therefore, there is no way to guarantee that the data is not tampered with without having an integrity service to check the originality of the data. Imagine what could happen if a user were able to change his online order information after payment, or an intruder able to change delivery information. Therefore, including integrity services is an essential requirement for e-Business transactions.

3. ***Availability***: this refers to the accessibility of information and resources when they are needed by any authorised party. A key advantage for a company doing e-Business is being available to its customers and partners all the time. This makes the existence of a service to ensure availability essential for successful e-Business (Outeye, 2003). A common interruption attack against availability is a Denial of Service (DoS) attack which can cause big financial losses. It can target the company communication infrastructure or application servers and render them permanently or temporary inaccessible, which can negatively impact on business, customers and partners.

4. ***Authentication***: Authentication is how to verify and ensure that the user is who he claims to be. The purpose of the Authentication service is to verify the identity of a user requesting access, for example by the mean of user ID and password, which although the simplest way is unfortunately the weakest and easiest to break. Authentication can be achieved by something you know, for example password or key, something you have, such as a smart card, your physical qualities, like biometrics ID (such as fingerprint or retina), or by location (you are authorised to receive mail from the postman if you simply open the front door of the mail's address!).

5. ***Authorisation***: Once a user has been authenticated to the system, the system needs to authorise the user, i.e. to determine which system resources the user is allowed to access and what set or actions he is allowed to perform on those resources. Authorisation is all about Access control, where all the system resources that the legitimate user is allowed to access are specified, along with a set of actions that he can perform on these resources. The Access control service assumes that the user has been successfully authenticated by the proper Authentication service.

6. ***Non-repudiation***: Requires that neither sender nor receiver of the message be able to deny the transmission (Stallings, 1998). It is important in e-Business transactions to be able to confirm any action and by whom this action has been taken. Such a security service is very important in case of dispute or liability when there is a need for proof of transactions.

7. ***Auditing***: Security services need to be integrated to maximise the level of protection. Based on that, Access control can be coupled with Auditing mechanism. A good Auditing mechanism allows the system to log all the relevant activities and access requests to its resources, and keep these logs for later verification. In a more complex situation, it enables a real-time analysis of all access requests and generates an automatic response based on that. Auditing also helps as deterrent mechanism: if the user knows that all his actions on the system resource are being logged and can be verified against any violation or malicious act, this will definitely stop him thinking about misusing the granted privileges.

We can also think about security in term of *prevention*, *detection* and *recovery*. For example, providing a clear security policy combined with a policy enforcement mechanism ensures the existence of a proactive way to prevent any accidental or deliberate misuse of the system. Detection mechanisms detect any potential security breaches. An example of a detection mechanism is Intrusion Detection Systems (IDS) which detects any abnormal activities in the network, logs these activities and sends an alert to the responsible authority in the system. Recovery ensures continuity and availability characteristics of the system. If a web service goes down because the server hosting the web contents crashes, a redundant web server which has the same content should be in place to recover this service. The recovery mechanism guarantees that the system will not deviate from its standard behaviour.

2.5 The Nature of e-Business Security

It is obvious that the Internet is the backbone of e-Business. However, Internet security always comes as an afterthought. This might be because of the nature of the Internet. Historically, the Internet was not for commercial use. The main purpose of it was information sharing and remote computer access. Therefore, simplicity and ease of use lay behind the open non-secure design of the Internet (Longstaff, et al., 1997). After the Internet evolved and became commercialised, many new Web application techniques (over the Internet, intranet, extranet) were developed. Users and even software developers were unaware of the security problems inherited from the open non-secure design of the Internet. This led to the creation of a vulnerable Web environment which can be maliciously exploited (Otuteye, 2003). As in most information and communication systems

technologies which have been developed, security comes as afterthought. This leads to an increase in the cost and complexity of achieving secure e-Business (Jiwnani and Zelkowitz, 2002) as well as increasing the chance of contradiction between security and system functionality (Baskerville, 1992). This may explain why security tries to catch up and why security practices need to be integrated with the e-Business systems lifecycle from the early stages in order to increase the level of security.

Moreover, e-Business systems have interconnecting and interacting components (people, software, hardware, procedures and data) and should be viewed from an Information System (IS) perspective, with a technological infrastructure and organisational framework, rather than as a pure technological infrastructure (Katsikas et al., 2005). Unfortunately, this complex socio-technical view is rarely captured by traditional security approaches (Siponen, 2005a). Results from many information security surveys show the diversity of information security issues facing e-Business adopters. For example, a survey which was conducted to identify the top information security issues gives a list of 25 issues that were considered by security experts as the most important information security issues facing organisations (Knapp, et al., 2006). These issues show us how much diversity and complexity is inherited in e-Business security:

- Top Management support.
- Malware (e.g., viruses, Trojans, worms).
- User awareness, training and education.
- Policy related issues (e.g., enforcement).
- Organisational culture.
- Standards issues.
- Vulnerability and risk management.
- Access Control and identity management.
- Governance.
- Legal and regulatory issues.
- Network security architecture.

Security is no longer an add-on feature, and since there is a huge demand for deploying Internet technologies for conducting e-Business, security needs to be integrated from the early stages of any e-Business project. The complexity of the e-Business environment makes understanding the security problem a difficult task. It is not enough to address only technical requirements to ensure confidentiality, integrity and availability, in order to raise the security bar. Organisations focus heavily on technical measures in order to protect their online business. However, many security statistics show us that these isolated technical measures fail to secure e-Business and the number of information security incidents continues to rise. According to UK national statistics, in 2005 more than 50% of UK businesses had e-breaches (UK national statistics, 2005). In 2007, the US companies' average annual loss due to security breaches was $350,424, from $168,000 the previous year (CSI, 2007). Although there is a notable technological evolution of security systems and mechanisms, every day the media publish news about information security breaches, and cybercrime, fraud, identity theft and credit card misuse are increasing dramatically. This gives us a reason to believe that traditional security approaches and ad-hoc security solutions are insufficient to thwart the increasing number of security breaches. These approaches, which perceive security from one dimension, are unable to provide adequate security levels for today's business environment and the large number of security breaches that we see every year provides evidence that encourages us to change and investigate other approaches that perceive security as an integrated part of business in the first place, and then follow a new way of understanding and solving the e-Business security problem.

2.6 The need for a socio-technical approach to e-Business security

The term "*Socio-technical*" is frequently used in the information security literature without a clear foundation; it mainly refers to approaches and methods which try to go beyond the technical dimension when dealing with the issue of securing information and communication technologies (Dhillon and Backhouse, 2001; Siponen 2005b). On the other hand, this term has stronger foundation within the management literature where it originally emerged. The term can be traced back to the 1950s when a number of field studies conducted by Tavistock institute in London and led to the development of socio-technical theory. These studies looked at the reasons behind the miners' stress, low moral and other psychological issues created when the British coal industry introduced new technology

(Trist and Bamforth, 1951). According to Mumford(1994) these studies were seminal and one of the important socio-technical principle formulated by them "is that if a technical system is created at the expense of a social system the results obtained will be sub-optimal...when work is being designed the goal must always be the joint optimization of the social and technical systems"(p.304). This research led to the development of work design principles which became very popular in the management field to increase employees' participation, to improve performance and to improve job satisfaction.

Later, similar ideas, which seemed to be influenced by the original socio-technical perspective, have started to emerge within the Information System (IS) research studies. These studies emphasized participatory approaches to increase the chance of developing and implementing successful IS projects. Several IS development methodologies can be described as socio-technical methods; this include ETHICS (Mumford, 1979), Soft Systems methodology (Checkland, 1981) and Multiview (Avison & Wood-Harper, 1990). However, the concept is usually used as an umbrella term to refer to methods, approaches and studies which gives an equal importance for both technical system and its social context. It emerged as a strong reaction to the predominant technical perspective which gives less attention to the human and organisational aspects surrounding the technical system.

As discussed in the previous section, this study views e-Business from an IS perspective. Iivari and Hirschheim (1996) distinguish between two IS views; the technical versus the socio-technical. A *technical view* "regards an information system predominantly as a technical artifact, and assumes that its connections with its organizational environment can be reduced to well-defined inputs and outputs and ergonomic interface questions" (p.153). On the other hand, a *Socio-technical view* "is based on the assumption of interdependent subsystems, the technical subsystem and the social subsystem which are designed jointly" (p.153). From the IS technical view users have no active role in developing secure information systems; in contrast, in the socio-technical view users may have a moderate influence on many information systems security activities, for instance, the information security requirements can be modified to meet the users' preferences (Siponen, 2005b).

Although the technical view of security is predominant in the literature of information systems security, several security researchers have recently started to call for more socio-technical approaches which are needed to overcome the limitations of the traditional ones

(Baskerville, 1992; Dhillon and Backhouse, 2001; Siponen 2005b). After analysing the major information security development methods, Baskerville (1992) concluded that these conventional methods fail to involve unqualified user participation in the security design process. Also, he noted that security methodology is still lagging behind the IS methodologies which started to consider the social context of technical artifacts developed using these methodologies. Dhillon and Backhouse (2001) conducted a major review to identify the current research directions in the information security domain and noticed a shift from a narrow technical view to a socio-organisational perspective. In their review, the majority of security models and approaches were classified under the functionalist paradigm which views the social world as a combination of concrete artefacts. Dhillon and Backhouse (2001) believed that this leads to security being treated as a something concrete which only fits military contexts, where this model was originally generated; however, in modern business organisations it is difficult to create such objective reality and consider information system and organisation as completely concrete entities. Consequently, they emphasised that security needs to move forward by adopting interpretive approaches:

> An interpretivist understanding of information systems security concerns certainly offers advantages, furnishing a holistic view of the problem domain, especially within the scope of networked organizational forms, instead of the simplistic, one-dimensional, explanation, more suitable for hierarchically structured organizations. At the same time interpretive approaches lack any prescriptive component and therefore offer value to a security manager (Dhillon and Backhouse, 2001, p. 141).

Recently, a review of modern information security approaches (Siponen, 2005b) showed a similar trend towards socio-technical information security thinking and highlighted the need for more empirically grounded security research. Few researchers have recognised the usefulness of such approaches in the field of information security or have made a real contribution in this direction (Kowalski, 1994; Yngstron, 1996; James, 1996). Recent literature supports the idea of managing security from a socio-technical perspective (Wimmer and von Bredow, 2002; Zipkin, 2005; Tarimo, 2006; Bakari, 2007; Zuccato, A. 2007). This rest of this section will provide a critical review of these studies in an attempt to identify the various dimensions affecting security, and will then formulate a conceptual framework which will guide the inquiry of this study. Table 2.2 summarises the studies

which have been reviewed. It shows in which context the study has been conducted, the different perspectives which were considered, its levels, and application of the study.

Table 2.2: Summary of reviewed studies.

Perspective	Study
- Technical	Kowalski, 1994; Yngsrtröm, 1996; James, 1996; Wimmer & von Bredow, 2002; Zipkin, 2005; Zuccato, 2007; Tarimo, 2006; Bakari, 2007.
- Managerial	Kowalski, 1994; Yngsrtröm, 1996; James, 1996; Zipkin, 2005; Zuccato, 2007; Tarimo, 2006; Bakari, 2007.
- Political	Kowalski, 1994; Wimmer & von Bredow, 2002.
- Legal	Kowalski, 1994; Yngsrtröm, 1996; Wimmer & von Bredow, 2002; Zipkin, 2005; Zuccato, 2007; Tarimo, 2006; Bakari, 2007.
- Ethical	Kowalski, 1994; Yngsrtröm, 1996; Wimmer & von Bredow, 2002; Zipkin, 2005; Zuccato, 2007; Tarimo, 2006; Bakari, 2007.
- Cultural	Kowalski, 1994; Yngsrtröm, 1996; Wimmer & von Bredow, 2002; Zipkin, 2005; Tarimo, 2006; Bakari, 2007.
- Operational	Kowalski, 1994; Yngsrtröm, 1996; Tarimo, 2006; Bakari, 2007.
Level	
- Individual	Kowalski, 1994; Yngsrtröm, 1996; James, 1996; Zipkin, 2005.
- Organisational	Kowalski, 1994; Yngsrtröm, 1996; James, 1996; Zipkin, 2005; Zuccato, 2007; Tarimo, 2006; Bakari, 2007.
- National	Kowalski, 1994; Wimmer & Bredow, 2002; Zipkin, 2005.
- International	Kowalski, 1994.
Application	
- IT systems	Kowalski, 1994.
- IT security education	Yngsrtröm, 1996.
- Healthcare system	James, 1996.
- e-Government	Wimmer & von Bredow, 2002.
- Computer viruses	Zipkin, 2005.
- e-Commerce	Zuccato, 2007.
- Security Readiness	Tarimo, 2006.
- ICT in Public Sectors	Bakari, 2007.
Context	
- Developed countries	Kowalski, 1994; Yngsrtröm, 1996; James, 1996; Wimmer & von Bredow, 2002; Zipkin, 2005; Zuccato, 2007.
- Developing countries	Tarimo, 2006; Bakari, 2007.

Kowalski (1994) proposed a Security by Consensus (SBC) model. The SBC model was intended to be a thinking aid to help in solving the problem of insecurity in information and communication systems. Kowalski introduced his socio-technical approach based on an interdisciplinary approach including general systems theory, sociology, criminology, computer science and information systems theory. He argued that a socio-technical system has four components: two technical (methods and machines); and two social (culture and structures). The overall socio-technical systems are striving for equilibrium between these components at all living system levels: individual, organisational, national and

international. The SBC model has been synthesised from studying four areas: ethics; politics and law; operations and management; and technology.

Based on general systems theory and Cybernetics - the science of communication, control and feedback - Yngström (1996) proposed a conceptual model called the Systemic-Holistic Model. It aimed to develop a better understanding of information security problems as they related to the original existing physical entities, on specific abstract levels and in specific contexts. Yngström used her model as a systemic-holistic approach for academic programs in the field of information security. She has demonstrated that the development of a holistic approach was most suited for academic IT security education.

The inefficiency based on rigid scientific methods that do not consider human factors, such as user participation, management responsibility, and support in traditional security planning and management methods, led James (1996) to suggest a more holistic and proactive approach for managing and selecting security measure within an organisation. This approach emphasised integrating information security with organisational objectives and mission, thereby building a holistic view for information security that has a proactive stance and increases the security culture within an organisation. To test her approach she implemented it within a private healthcare organisation.

Comparing these three previous approaches (Kowalski, 1994; Yngstrom, 1996; James, 1996), we may feel they are similar. This is true in one way because all of them support the idea of holism for dealing with information security issues. However, James attempts to build security management strategy which focuses more on user and management participation, security awareness and culture. The strategy was for the one organisation where the study was conducted. This may raise the question about its applicability in other environments and whether it can be generalised or not. On the other hand, Kowalski and Yngstrom built conceptual models for understanding and dealing with information and communication systems security in general. They provide us with powerful thinking tools to view information security as a whole. This encouraged other researchers to adopt these two models as approaches for understanding the nature of the security issues in different environments which have their own technological and social characteristics. For example, Tarimo (2006) adopted the SBC model to develop a security readiness check list and Bakari (2007) employed both the SBC model and the Systemic-Holistic approach to propose a

holistic security management approach for public organisations. Both examples were in a developing country context and based on socio-technical approaches.

Another contribution in the field of e-Commerce security worth considering is the research done by Zuccato (2007) who followed a systemic thinking approach to build a holistic management framework which should be applicable in electronic commerce. Zuccato argued that most security management approaches that have been developed fail to consider the different dimensions affecting the e-commerce environment. Additionally, these approaches are not applied because they are considered complex and expensive. He also believed that many of these approaches do not take the changed environmental circumstances of electronic commerce fully into account. Based on that, he proposed a holistic framework for security management which aimed to allow organisations to conduct security management in an easy and cost-effective way that suits e-commerce systems. Zuccato suggested three sources of security requirements: Business, Technology and Society. These three sources form the basic dimensions of his framework. The framework has been implemented in a banking environment. A similar contribution has been made by Wimmer & von Bredow in the field of e-Government solutions. They argued that despite the similarities between e-Commerce solutions and e-Government solutions at the technical level, security requirements differ and hence e-Government security solutions need a socio-technical approach that considers political, cultural, and legal as well as technical impacts. One may agree that the security requirements vary between e-Commerce and e-Government; however, a socio-technical approach is necessary for both of them, and applying a pure technical approach in e-Commerce security is not enough for considering all the factors that affect e-Commerce environments. Even in e-Commerce, legal, cultural, ethical and political factors may affect information security. For example, e-Business/e-Commerce organisations will not survive if they break laws or do not consider the ethical, cultural and social requirements of their consumers (Chu et al., 2005).

In the e-Business domain, recent reviews of the body of research have identified the predominance of the technical view when dealing with e-Business security. Researchers have focused on the security problem from either the technical point of view, which is the common trend in this field, or from the managerial (Ngai and Wat, 2001; Wareham et al., 2005). Few studies follow multi-disciplinary or socio-technical approaches for handling the

security problem. Many studies related to e-Business security focused on the technical part of the problem (Williams, 2003; Nabi, 2005). Most of these studies discussed issues such as system level security, secure coding and configuration, communication links security, the use of cryptography and digital certificate. Other studies focused only on the managerial and the legal aspects of information security (Sundt, 2006; McConnell, 2006). Others discussed e-Business requirements without taking care of security at all (Dezelak et al., 2006). This scarceness of socio-technical studies limited our understanding of the diverse issues affecting e-Business security. According to Kajava et al., (2007) attention was on technology and information networks when people talked about security; however, other issues such as individuals, organisation and management become increasingly important. Kajava stressed that information security is a strongly cultural issue – especially when e-Business is to be expanded into different geographical areas where cultural norms, habits and values differ.

2.7 Conceptual framework of enquiry of this study

Based on the stakeholder model suggested in section 2.3 and the IS socio-technical perspective adopted in section 2.6, e-Business is viewed in this thesis as a complex socio-technical system with three interacting elements; stakeholder, enabling technology and business process. Based on this foundation, this study will use a conceptual framework to guide its enquiry for exploring the different dimensions influencing security in e-Business environments. As shown in Figure 2.4, this framework is a multidimensional one; each dimension has its own characteristics and components which may affect the other dimensions or be influenced by them. These dimensions have continuing interactions with each other, therefore, they need to be explored in relation to each other and in relation to the relevant stakeholders in the e-Business environment. The framework has a social dimension, with human, organisational and legal components which interact with the information, processes, and infrastructure components embedded in the technical dimension. Each one of the previous dimensions could have a significant effect on e-Business security. For instance, security issues could emerge from the vulnerabilities in the components of the technical dimension, or they could result from interaction between the components of the social dimension and the components of the technical dimension.

Giving the inductive nature of the study these dimensions are defined at an abstract level to allow a more flexible way to explore the problem in relation to its context. At a later stage, grounding this framework within the study findings will help us to identify and understand the actual factors affecting the e-Business security environment.

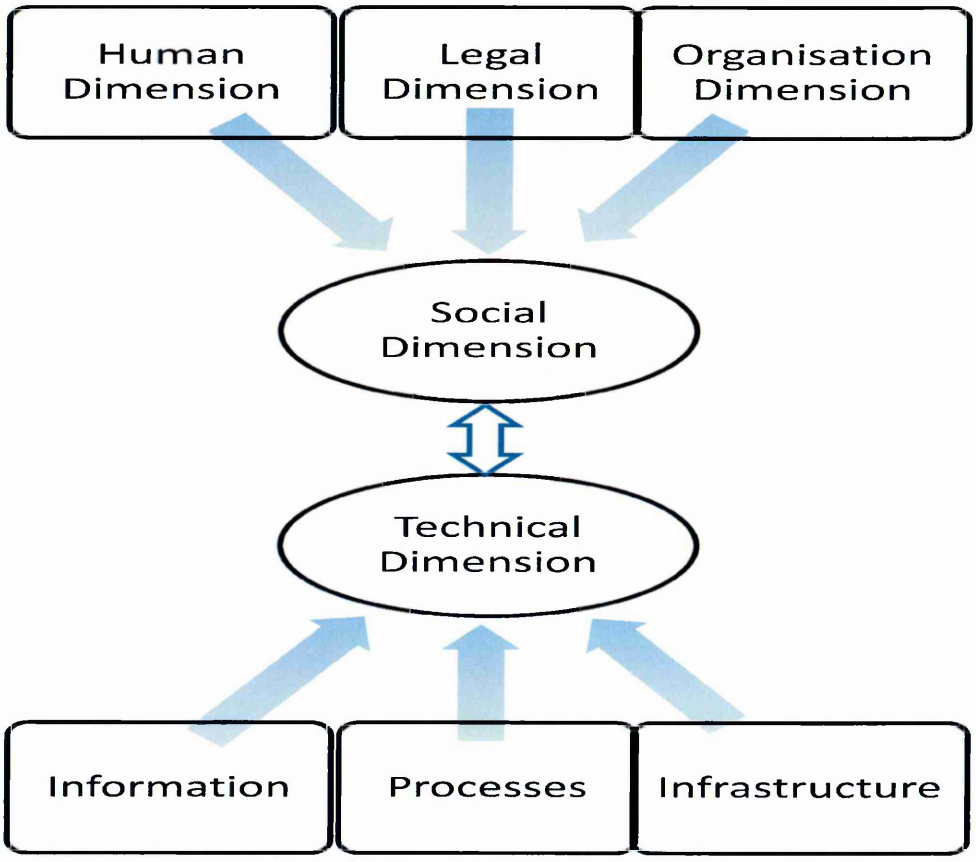

Figure 2.4: A socio-technical framework of enquiry for e-Business security

The Technical Dimension is concerned with providing technical security mechanisms in order to protect three primary components - information, processes, and infrastructure - owned/needed by a particular stakeholder to utilise e-Business. From a technical viewpoint, requirements such as encrypted communication channels, protected databases, physical and logical access control, and user identification, are essential for a secure e-Business environment. This dimension is concerned with the technical mechanisms which are required to implement the basic security services discussed in section 2.4.2.

The Organisational Dimension is concerned with developing secure environments that support and enforce the technical solutions in place. Within e-Business organisation, this

dimension focuses on how issues such as culture, structure, responsibility, stakeholders' interactions and perceptions can affect security. It also emphasises requirements such as organisational security policies, procedures, guidance and engagement from people at all levels of the organisation, from top management down to the employees.

The Human Dimension is concerned with the effect of human factors on the effectiveness of existing security mechanisms and procedures. The interaction between this dimension and the technical dimension implies that the security mechanism should be usable and psychologically acceptable in a way that reduces the risk of security breaches which are a result of human errors or omissions. Moreover, because of human factors such as habits, culture, norms, knowledge and perception, this dimension views people as a weak link in the security chain and strives to strengthen this link by providing the necessary requirements to help people to take better security decisions and to prevent accidental or intentional abuse of e-Business information, processes and/or infrastructure.

The Legal Dimension is concerned with developing an effective legal framework that regulates e-Business activities and recognises their associated security aspects. It focuses on the legal conditions which are necessary to protect e-Business stakeholders and encourage them to participate in an e-Business environment with greater confidence. It views government as an important stakeholder whose effect could span a wide range of stakeholders and security aspects. It also speculates that government involvement in e-Business security could affect several security dimensions, including technical and organisational as well as legal dimensions. It may cover issues such as online contracting, the legal power and authenticity of electronic documents, recognition of electronic signatures and digital certificates, prevention of cybercrime, and privacy protection.

2.8 Summary

This chapter has served several points. First, it set out the study's terminology by defining and discussing the basic terms, concepts and issues associated with e-Business and information security. Accordingly, e-Business is viewed as a complex socio-technical system with three interacting elements; stakeholder, enabling technology and business process. With respect to this complex view, the literature review showed that few stakeholders apart from customers and internal organisation are likely to be considered, and

this significantly limits our understanding of the role and the effect of other important stakeholders such as governments and technology providers. To fill this gap, stakeholder analysis is proposed for use as an organising principle in this research. Therefore, the stakeholder concept was discussed and placed within the problem domain to form a foundation for the study's conceptual framework.

Additionally, this chapter presented the current trends in information security research including e-Business security research. It found that a great deal of research work in security has focused on producing theoretical models or technical solutions without addressing the real world where research outcomes are supposed to be used. In response to the limitations of these technical approaches towards security, the literature review identified a paradigm shift toward a socio-technical perspective which is much needed in today's complex e-Business environment. It called for more socio-technical information security thinking and highlighted the need for more empirically grounded security research. As a contribution to this emerging body of research this study adopts this perspective as an underlying assumption for its inquiry which will help in identifying and better understanding the various dimensions affecting e-Business security environments.

In the light of the proposed stakeholder model and the adopted security perspective, the problem situation in the context of the study was justified. Various aspects of the problem of e-Business security were identified and limitations of the previous studies in the same context were discussed. While these previous studies raise our intentions towards e-Business security in the context of the study, they do not capture the complexity of the problem domain nor develop knowledge and/or understanding of the various associated issues and stakeholders. This encouraged the researcher to develop a better research design to fill the existing research gap.

Based on the above, a conceptual framework guiding the study inquiry was proposed. By combining the previously discussed socio-technical perspective and stakeholder analysis with a well-designed knowledge-generating approach, a holistic understanding of e-Business security in the context of the study is likely to be developed. Such an understanding can be extended to generate better ideas to deal with the multifaceted nature of the e-Business security problem.

Chapter 3 : Methodological Considerations

Considering the multifaceted nature of e-Business security discussed in the previous chapter and the characteristics of e-Business as a complex emerging Information System (IS) field, this study follows an interpretive research approach to develop a better understanding of the e-Business security environment. Within the context of IS, interpretive methods of research are "aimed at producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context" (Walsham, 1993, pp. 4-5). Although interpretive research has become a well-established part of the IS field (Klein & Myers, 1999; Walsham, 1995, 2006), it has just recently started to gain ground in the field of information security (Bolan & Mende, 2004; Siponen & Oinas-Kukkonen, 2007). Being characterised by considering phenomena in their natural settings, the interpretive approach to e-Business security gives the possibility of understanding the influence of the social and organisational aspects of the context in which technical systems operate (Kaplan & Maxwell, 1994).

Thus, in this chapter the researcher argues for the suitability of and the need for a more inductive interpretive approach and qualitative research method to investigate e-Business security. The methodological considerations in the process of selecting a suitable research method for this study are discussed. After identifying the research assumptions underlying each available research method and assessing their potential for this study, a justification of the selected research method is given; this is followed by a complete research design including research strategy, data collection techniques, and analysis procedure.

Selecting an appropriate methodology for e-Business security depends on several factors (Trauth, 2001). Among the important ones are the nature of the problem under investigation, the complexity of its environment, and the researcher's theoretical lens. Before discussing these factors in relation to our problem area, the next section discusses the underlying philosophies or paradigms of research methodologies that researchers should consider when selecting a methodology for conducing research study.

3.1 Underlying Paradigms

A paradigm means a set of common shared assumptions or way of thinking about reality (Oates, 2006). Research paradigms identified by researchers are based on two main philosophical assumptions (Myers, 1997): ontological assumption, concerned with how we view the world; and epistemological assumption, concerned with knowledge and how it can be acquired. Accordingly, three paradigms have been identified in studies related to information systems (Orlikowski & Baroudi, 1991): positivist, interpretive, and critical paradigms.

Positivist research can be generally characterised as a theory- or hypothesis-testing research (Myers, 1997). In terms of direction between realty and theory, it is a deductive research which starts from the conceptual world with theory and then tests it empirically in the real world. Ontologically, it perceives the world as a series of fixed and measurable phenomena that can be objectively and repeatedly observed and investigated with structured instrumentation independently from the researcher (Chua, 1986). Positivism has it origin as the underlying philosophical assumption for natural sciences such as physics, chemistry and mathematics; however, positivist methods of research have been adopted and used extensively in many other fields.

Interpretive research emphasises the role of people and how they interact with the phenomenon under investigation. According to (Chua, 1986), "interpretive studies assume that people create and associate their own subjective and intersubjective meanings as they interact with the world around them...the intent is to understand the deeper structure of a phenomenon...to increase understanding of the phenomenon with cultural and contextual situation". It does not seek to test a hypothesis: instead, it aims to create a holistic understanding of a phenomenon by identifying, exploring and explaining how all the factors in the social context of the phenomenon are related and interdependent (Oates, 2006). The intent is not to generalise from the setting to a population; rather, the intent is to develop a deeper understanding of the structure of a phenomenon, which it is believed can then be used to inform other settings (Orlikowski & Baroudi, 1991).

Critical research aims to critique the existing state of affairs (Chua, 1986). It is based on the assumption that social reality is historically established and that it is produced and reproduced by people (Myers, 1997). It tries to uncover conflicts, oppositions and contradictions within the social systems. In relation to information systems study, critical research has been defined as concerned with power relations, conflicts and contradictions, and empowering people to eliminate them as sources of alienation and domination (Oates, 2006).

However, the predominance of the positivist paradigm in IS studies is notable. It has been argued that the domination of positivist studies has limited the aspects of information systems phenomena we have studied, and how we have studied them. Consequently, "this has implications not only for the development of theory and our understanding of information systems phenomena, but also for the practice of information systems work" (Orlikowski & Baroudi, 1991).

A similar situation can be observed in information security studies. Research in the realm of information security has its roots in computer and engineering sciences (Yngstrom & Bjorck, 1999; James, 1996). Therefore, approaches to information systems security have been based solely on a positivist paradigm of the natural sciences with the assumption that since the world is ordered, regular, and not random, we can investigate it objectively (Oates, 2006). However, it has been argued that this is no longer valid to be applicable in the field of information security:

> The times when the whole body of IT knowledge could fit into the finite domain of computer science are gone forever. Today, ethical, social, legal and economic implications of IT use must be considered - so also within the realm of information security (Yngstrom and Bjorck, 1999, p. 2).

When security has evolved to include diverse issues with strong social foundations, positivist-based approaches alone cannot offer the flexibility and the possibility to explore the influences of interacting social elements on the security environment. Applying the reductionism concept of the positivist paradigm in such a situation means missing the bigger picture (Oates, 2006), and thus, the lack of holism, which could be one of the reasons why security is usually overlooked, comes as an afterthought, or is perceived from a purely technical dimension.

This critique of the positivist paradigm makes the interpretive paradigm a potential candidate for this study. This can be justified by comparing the socio-technical nature of the study's inquiry with the underlying assumptions of interpretive philosophy. The study purpose is to understand a complex phenomenon, namely, e-Business security in the context of Jordan. According to Newman et al. (2003), in a typology of research purposes, understanding complex phenomena (understanding phenomena, understanding culture, understanding change and understanding people) can be taken further to generate new ideas (exploring phenomena, generating hypotheses, generating theories, uncovering relationships, uncovering culture, revealing culture). In the previous chapter we have identified the problem situation[2] by constructing a framework of enquiry that views the problem in relation to several interrelated dimensions (see figure 2.4). Here we have a complex and dynamic situation in which we seek to develop a holistic understanding of e-Business security in relation to its context as well as considering all the stakeholders in the problem situation. Understanding the interaction of the components of the social dimension with the technical dimension would create more opportunity for securing the e-Business environment. This inductive nature for the study purpose makes the interpretive paradigm more appropriate to such an inquiry as it is a knowledge-generating approach.

As for the critical paradigm which aims to reveal and critique contradictions and seek emancipation, this does not match with the aim of our study, therefore it is considered inappropriate for our study.

3.2 Research Approaches: Qualitative vs. Quantitative

The answer to the question whether to use qualitative or quantitative research methods is not straightforward. In this section these two common research classifications and the assumptions that separate and influence the choice of a particular research approach will be discussed.

Quantitative research methods are based on positivist philosophy and have their roots in the natural sciences such as physics and mathematics. However, quantitative research methods such as surveys and mathematical modeling are now well accepted in social sciences

[2] In a complex situation such as e-Business security the term "problem" is inappropriate. *"There will be many problems, hence the term "problem situation"- a situation in which there are perceived to be problems"* (Wilson, 1990).

(Myers, 1997). Quantitative research methods are deductive in nature and better suited for theory testing (Lee, 1998). On the other hand, qualitative research methods have their roots in social science; however, the general shift in information systems from focusing on technical issues to managerial and organisational issues increases the interest in application of qualitative research (Myers, 1997). Although many researchers argue that qualitative research methods are inductive and are usually used for hypothesis generation (Lee, 1998), other researchers believe that, while quantitative research can be only positivist, a qualitative approach can be based on any research paradigm discussed previously (Straub et al., 2004). See figure 3.1.

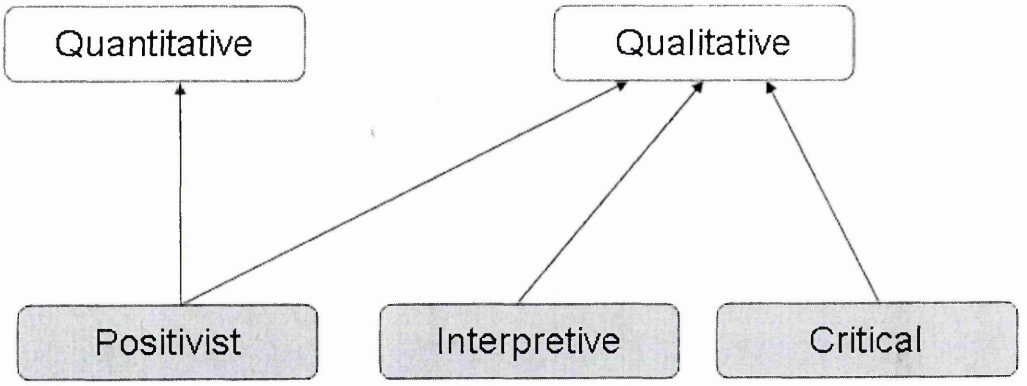

Figure 3.1: Epistemological Assumptions for Qualitative and Quantitative Research (Straub et al., 2004).

The difference between quantitative and qualitative approaches is too often regarded as "numbers versus no numbers" (Lee, 1998). Unfortunately this is oversimplified, and many researchers point out several fundamental differences (Creswell, 1994; Kavel, 1996). Lee (1998) summarises these differences as following:

- **Qualitative research**: is inductive, theory-generating, subjective and non-positivist inquiry.
- **Quantitative research**: is deductive, theory-testing, objective and positivist inquiry.

Selecting interpretive philosophy as a theoretical lens for this study implies that qualitative research methods are the appropriate methods to choose to fulfil the purpose of our study. In the next section the suitability of a qualitative approach for the purpose of this study is justified.

3.3 Suitability of Qualitative Methods in the field of e-Business Security

Our discussion of the suitability of qualitative approach is based on the factors discussed by Trauth (2001) that influence the choice of qualitative methods in information systems research. The researcher believes that among these factors, three are relevant for this study: the nature of the research problem; the researcher's theoretical lens; and the degree of uncertainty surrounding the phenomenon.

3.3.1 The nature of research problem

Trauth (2001) argues that "the nature of the research problem should be the most significant influence on the choice of research methodology". In our case the research problem is concentrated around e-Business security in the context of Jordan. The study seeks to answer the question of how security can be incorporated in the problem situation to provide a trustworthy e-Business environment which considers the needs and requirements of e-Business security stakeholders. Based on the nature of the research question, the interpretive qualitative approach was chosen as an epistemological and underlying assumption for this study. Arguably, two reasons make this approach appropriate in our research. First, the exploratory nature of the study requires the use of an approach which provides a deeper understanding of the research situation and which could lead to the generation of new ideas that can help to overcome the problem associated with e-Business security. This is best achieved through a knowledge-generating approach such as an interpretive qualitative one. Second, by adopting the stakeholder notion in this research, it allows us to explore all the interested parties in the study environments and investigate their interrelationships and interactions in the e-Business environment. Such stakeholder analysis necessitates a holistic approach which perceives the problem in relation to its context; hence, reinforcing the choice of qualitative approach.

3.3.2 The researcher's theoretical lens

By theoretical lenses Trauth (2001) means the underlying epistemologies used to frame the study. These are the positivist, interpretive and critical paradigms discussed previously. The traditional security approach has been criticised for being purely technical and based upon positivist methods of research that are not suitable for human related systems environments (James, 1996). Accordingly a socio-technical perspective based on interpretive assumption is adopted in this study and forms a foundation for its enquiry. A socio-technical approach to e-Business security is better achieved through an interpretive understanding of security within its natural setting (Dhillon & Backhouse, 2001). An interpretive approach is more suitable for understanding the challenges in information security culture since its research methods can comprehend the behaviour of individuals in relation to information security practices (Zakaria, 2004). Interpretive based methods offer an integrated view of the context under investigation and capture the perceptions of the local actors (Miles & Huberman, 1994) which are fundamental from a socio-technical perspective.

3.3.3 The degree of uncertainty surrounding the phenomenon

Trauth (2001) also points out that the amount of uncertainty surrounding the phenomenon under investigation is considered an important factor in the choice of qualitative research methods. While the previous studies presented in Chapter 2 highlighted e-Business security problems in the context of the study, yet, aspects of these problems are not explored nor explained in detail, leaving a considerable level of uncertainly. For instance, questions such as how the different stakeholders perceive and interact with e-Business security and why security is addressed in a particular way within the context of the study need to be answered. Given this complex and uncertain situation with a wide range of interacting stakeholders and dimensions impacting on e-Business security, a qualitative approach provides an appropriate way for capturing this complexity and uncovering the uncertainty.

3.4 Qualitative Research Strategies

A research strategy means a particular research method to be applied in a specific research study. A research method is a strategy of inquiry based on a particular philosophical assumption which guides the process of research design and data collection (Meyers & Avison, 2002). Several research strategies found in the literature are classified as qualitative

research methods. For example ethnography, case study, action research, and grounded theory are all qualitative methods used in information systems and organisational related studies (Cassell & Symon, 2004; Myers, 1997).

In this study, the case study research method has been adopted as a strategy for guiding its inquiry and data collection procedures. In IS research, interpretive case study is considered a well-established qualitative research method which enables the researcher to "examine phenomena in its natural setting, employing multiple methods of data collection to gather information from one or a few entities (people, groups, or organizations)" (Benbasat et al. 1987, p. 370). Its powerful characteristics and ability to fit different research settings encouraged many researchers to use it in their studies. For instance, Zakaria (2007) has employed in-depth case study to investigate information security culture challenges in a Malaysian public sector organisation. In another study, interpretive case study was used by Dhillon (1995) to analyse information security management in two large British organisations. Other researchers have combined case study with other qualitative strategies. For instance, Trauth (2000) has used a country-based case study and ethnography to study the socio-cultural influences on the information economy of Ireland. Another researcher has applied case study and grounded theory research methods to develop a framework for conceptualising the organisational issues around the adoption and use of CASE tool (Orlikowski, 1993).

The lack of a clear procedure for analysing qualitative data within the case study method seems the reason behind combining it with other qualitative strategies which provide systematic analysis procedures. In contrast to case study, both General Inductive Approach (Thomas, 2006) and Grounded Theory (Strauss & Corbin, 1990) guide the researcher in the process of analysing and interpreting the data collected during the field study. In the current research, case study method is combined with a general inductive approach realised through thematic framework analysis. This analysis approach will be discussed in more detail in section 3.6.3 as part of the study research design.

The next section will discuss the principles of applying case study research method and its suitability for investigating e-Business security in the context of this study.

3.5 Suitability of Case Study Strategy in this Research

Case study is one of the common research strategies in information systems studies (Orlikowski & Baroudi, 1991). It is argued that the case study research method is suitable for studies which require deep understanding of social or organisational processes because of the rich data collected in context (Hartley, 2004). Case study research is also defined as "an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" (Yin, 2003, p. 13). Thus, the need for a case study research strategy emerged from the fact that the phenomenon under investigation is too complex to be understood in isolation from its environment. Benbasat et al. (1987) discussed three reasons which render the case study method a valuable research strategy in information systems research:

1. Theory generation based on studying information systems in their natural setting and learning about the state of the art in the practical field.
2. Answering "how" and "why" questions that seek to understand the nature and complexity of the processes taking place.
3. Researching new areas and emerging topics where few previous studies have been carried out.

Accordingly, the aim of study and the research question(s) that it tries to answer are significant factors for considering the case study method (Benbasat et al., 1987; Stake, 1995; Yin, 2003). This study inductively tries to develop a holistic understanding of e-Business security in Jordan, the issue which has been regarded by many previous studies as a major barrier to adoption of e-Business, but unfortunately never explored in detail. It aims to answer the question of "*why*" it is usually overlooked, comes as an afterthought or is perceived from purely technical point of view, through understanding the question of "*how*" the different stakeholders perceive, interact with, affect and are affected by the e-Business security environment. In order to construct such a rich holistic picture the researcher believes that case study is an appropriate strategy that fits the nature of this research which tries to generate knowledge about a contemporary issue in its natural setting.

3.6 Research Design and Units of Analysis

This section presents the overall plan for conducting this research study. The plan represented in Figure 3.2 shows the research design, which is "the logical sequence that connects the empirical data to a study's initial research questions and, ultimately, to its conclusions" (Yin, 2003; p. 20). The research design is provided to ensure a systematic way of achieving the objectives of the study and to avoid the situation in which the gathered evidence does not address the research questions.

The research aims to develop a conceptual framework for understanding the e-Business security problem in the context of Jordan based on an interdisciplinary inquiry which considers technical and non-technical aspects of e-Business security. For this purpose, and based on the literature review, a conceptual framework to guide the study inquiry has been identified. The framework of inquiry defines a set of abstract dimensions and stakeholders of e-Business security to ensure that the problem area will be addressed holistically. Based on the research aim and the literature review and with the guidance of a framework of inquiry, four research questions (Q1, Q2, Q3 and Q4) were defined. Answering these research questions will lead to answering the general research question of the study (Q5). See figure 3.2.

Based on the nature of the research questions, an interpretive qualitative approach has been chosen as an epistemological and underling assumption (theoretical lens) for the study. The selection of Jordan as a problem situation has led to the application of a single case study with multiple embedded units of analysis as discussed by Yin (2003). At the macro level, Jordan was chosen as a country-based case study. This choice (country level case study) was guided by the framework of inquiry presented in Chapter 2 in order to focus on the social aspects in relation to the technical aspects and their relationships with e-Business security in the country. This would provide a sufficiently rich and focused study. At the micro level, and based on the stakeholders model discussed in Chapter 2, four units of analysis have been chosen. These are: technology providers; e-Business organisations; customers; and government. This embedded design of the case study allows focusing the enquiry and avoiding the disadvantage of the holistic design of a single case study which may lead to investigating the case at an abstract level, lacking any clear measure or data (Yin, 2003).

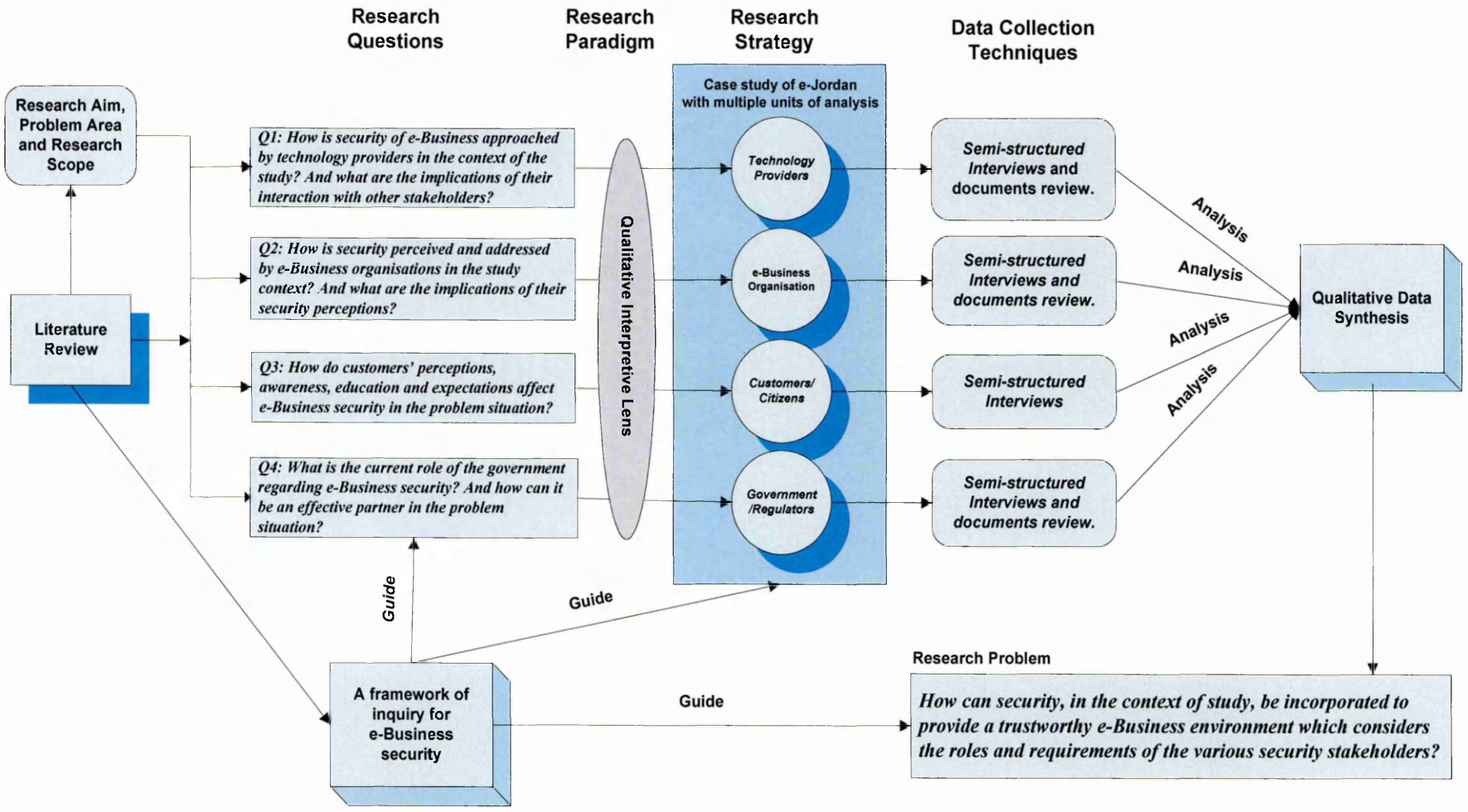

Figure 3.2: Research Design; the overall plan for conducting the study.

Methodological considerations of the selected units of analysis are discussed below, including sampling, data collection techniques, and analysis approach. Each subsection presents a theoretical background of the available techniques, followed by discussion of the particular procedures of each unit of analysis.

3.6.1 Sampling considerations

Sampling in qualitative research is totally different from quantitative sampling. While the later is characterised as a random process to select a representative sample from the study population, qualitative sampling tends to be purposive and aims to select a sample of participants that will help the research to achieve the study objectives (Miles & Huberman, 1994). The aim of qualitative research is to provide illumination and understanding of a complex phenomenon within a particular context. Hence, its findings cannot be generalised, but they are transferable, which means they can be applied to other contexts (Ryan et al., 2007). The fact that qualitative research does not seek generalisation renders random sampling an inappropriate technique for selecting participants in a qualitative study (Marshall, 1996).

Qualitative sampling is also characterised as an emerging process in which exact sample size and sampling techniques cannot be defined in advance; rather, they emerge during the process of conducting the research. This is due to the fact that the nature of units of analysis in qualitative research cannot be pre-identified, but is to be discovered (Luborsky & Rubinstein, 1995). This also implies an iterative process of data collection and analysis until reaching the "Theoretical Saturation" stage, which occurs when all of the main aspects of the phenomenon have been identified and incorporated into the emerging theory, model or framework (Guest et al., 2006).

To ensure richness in the collected data, qualitative study usually starts with a purposive sample of a small group of key participants who can provide information about the phenomenon in question (Ryan et al., 2007). This can then be followed by either snowball sampling or theoretical sampling. In snowball sampling, the initial participants recommend other potential participants who can provide additional insights into the research problem in hand (Marshall, 1996). After analysing the data collected from the initial participants, sample selection tends to be theory-driven in order to further develop and explain the concepts and themes emerging from the initial analysis; this type of sampling is known as

theoretical sampling which "continues until themes emerging from the research are fully developed, in the sense that diverse instances have been explored, and further sampling is redundant. In other words, patterns are recurring or no new information emerges; a situation sometimes referred to as saturation" (Fossey et al., 2002, p. 726).

In the context of this study, the researcher employed several qualitative sampling techniques in order to ensure an appropriate selection of participants, who can inform the study, and adequate sampling of information resources, thereby ensuring information richness which is required for addressing the study research questions and developing a full description of the e-Business security environment in the context of the study. In total, 58 participants representing different stakeholder groups took part in this study. Sampling within each unit of analysis is discussed below.

The study started with a purposive sample of three key informants representing major technology providers who were involved in several e-Business projects in the country. The choice of these three providers was based on the reasons that they are leading e-Business providers in the country and they provide most of the hardware and software required by local organisations to adopt e-Business. Background details of these providers and analysis of their security role in business environment are presented in Chapter 4. As a result of the themes which emerged from this unit analysis, further parties were identified as important stakeholders who may have great influence on e-Business security. Therefore, theoretical sampling was employed to further develop and explain these emerging findings. This led to the identification of an additional three units of analysis representing different stakeholder groups; e-Business organisations, customers/citizens, and government.

For the second unit of analysis, which aimed to explore the security role of e-Business organisation, a local airline company which undertook major transformations to adopt e-Business was chosen. Within this unit of analysis, which is presented in Chapter 5, several sampling techniques were employed, including purposive, snowball and theoretical. To achieve a holistic understanding of security in e-Business organisation, participants from different organisational levels were chosen to participate in this study (see Table 3.1). As the table shows, participants have various roles and responsibilities and are from different sections, which allowed the research to explore the problem from different angles and cover all its aspects.

The field study was conducted over a period of 6 months (April-September, 2008) and 28 participants were interviewed. Two or three site visits per week were arranged in collaboration with two IT members after getting agreement with the company's CIO. On the first visit, the researcher reviewed the structure of the organisation and tried to determine the key persons and the possibility of scheduling a time for interviewing them in a way that would not interrupt their work. After conducting a few interviews with key informants the researcher was able to identify further participants and arrange to interview them. The researcher was given a temporary desk at the IT department which allowed him to write his notes and observations or to review some related documents. He had access to the company for the full working day, allowing him to make visits to different departments and arrange to interview different people within the company.

Table 3.1: Sample within the second unit of analysis.

Participants positions	Count
IT Management	**9**
Chief Information officer	
Chief Security Officer	
Technical Support Manager	
IT Development Manager	
IT director	
IP Network Manager	
Help Desk Manager	
Help Desk Directors	
Departure Control System Manager	
Business Management	**4**
E-Business Director	
Credit Card Manager	
Human Resources Manager	
Legal Advisor	
IT Staff	**8**
Programmers (2)	
Systems Administrators (4)	
Networking Engineers (2)	
Non-IT staff	7
e-Marketing Staff (2)	
e-Business Staff (3)	
Finance Staff (2)	
	Total = 28

In the third unit of analysis, presented in Chapter 6, a purposive sample of Jordanian citizens was recruited to explore customers' security perceptions in the study context. Participants were chosen because they had previous experience with the Internet, whether they bought or sold online or just used the internet for online banking, communication and

searching for information. The researcher started with a convenient sample followed by a snowball sample in which the initial participants were asked to suggest other people who might participate in this study. Then the study followed a theoretical sampling technique to use as many samples as possible from the study environment until the researcher gained a deep understanding (theoretical saturation) of the customers' side of the problem. In total, 27 participants took part in this unit of analysis, including university students, personal contacts and users from internet cafés, which are very popular all over the country.

Finally the fourth unit of analysis focused on the security role of the government in the e-Business environment. For several reasons which will be discussed in the next section, document analysis was the primary source of data in this unit of analysis. Yet, purposive sampling was employed to select the appropriate information resources (government documents and legal sources) to inform the study. This unit of analysis is presented in Chapter 7.

3.6.2 Data collection techniques within case study method

Several qualitative data collection techniques and sources of evidence can be used in case study research. The most common techniques are interviews, observation/field study, documents and archives review and physical artifacts (Myers, 1997; Yin, 2003; Eisenhardt, 1989). Yin (2003) identified seven information resources that can be used in case study research. He also discussed the strengths and weaknesses of each source of evidence. These are presented in Table 3.2.

It is unlikely that the researcher will only depend on one data collection technique in conducting a case study (Eisenhardt, 1989). The use of multiple data collection techniques, commonly known as "data collection triangulation", is one of the important factors for establishing correct operational measures for the concepts being studied (Yin, 2003), therefore providing strong constructs and/or hypothesis (Eisenhardt,1989). While each data collection technique has its own particular strengths and weaknesses, triangulating more than one technique is likely to increase the strength and reduce the weaknesses of the overall data collection procedure.

Table 3.2: Case study sources of evidence: strengths and weaknesses (Yin, 2003).

Source of Evidence	Strengths	Weaknesses
Documentation	- Stable: can be reviewed repeatedly. - Unobtrusive: not created as a result of the case study. - Exact: contains exact names, references, and details of an even. - Broad converge: long span of time, many events, and many setting.	- Irretrievability: can be low - Biased selectivity if collection is incomplete. - Reporting bias: reflects the (unknown) bias of author. - Access: may be deliberately blocked.
Archival Records	- same as above - Precise and quantitative.	- Same as above. - Accessibility due to privacy reasons.
Interviews	- Targeted: focuses directly on case study topic. - Insightful: provides perceived causal inferences.	- Bias due to poorly constructed questions. - Response bias. - Inaccurate due to poor recall. - Reflexivity: interviewee gives what the interviewer want to hear.
Direct Observations	- Reality: covers events in real time. - Contextual: covers context of event.	- Time-consuming. - Selective: unless broad coverage. - Reflexivity: event may proceed differently because it is being observed. - Cost: hours needed by human observers.
Participant Observations	- Same as above. - Insightful into interpersonal behavior and motives.	- Same as above. - Bias due to investigator's manipulation of events.
Physical Artifacts	- Insightful into cultural features. - Insightful into technical operations	- Selectivity. - Availability.

A discussion and evaluation for each data collection technique is provided below, followed by a discussion of the particular data collection procedure used in each unit of analysis in the study.

Semi-Structured interviews: interview is considered the most common technique of data collection in qualitative research. The goal of any qualitative interview is to investigate the research topic from the perspective of the informants and to understand "how" and "why" they have this particular view (King, 2004). A common distinction is usually made between *structured* and *unstructured* interviews. Structured interviews have very specific objectives and a predefined set of questions which the interviewee should answer and at the extreme tends to be quantitative. On the other hand, unstructured interviews are open-ended in nature with no specific predefined questions; themes, issues and questions related to the topic emerge during the interview (Lee, 1999). The unstructured form seems to be more flexible; however, it is more costly and time consuming, therefore, many researchers

employ *semi-structured interview* (Seaman, 1999). Semi-structured interviews combine features from the two previous forms to get the advantages of both forms. Semi-structured interviews are usually designed to include overarching topic, general themes, targeted issues and specific questions with a predetermined sequence of their occurrence (Lee, 1999). Moreover, the interviewer is free to probe the interviewee for more information and unforeseen issues.

Direct observation: Direct observation is important for providing additional information about people in their natural setting and how they interact with technology and business activities which can increase the researcher's understanding of the problem being studied (Yin, 2003). As we can see from Table 3.2, there are two types of observation that the researcher can employ in his study. Direct observation seems more convenient than participant-observation because the latter requires the researcher to be an active participant in the problem situation: this means that the researcher must either be an employee in the unit of analysis or have permission to be an active participant in it. Because of the difficulty of fulfilling these requirements, especially with activities related to information security which are likely to be confidential, in additional to the time constrain, observation techniques were not used in this study.

Documents review: many types of documents can be potential sources of data in case study research. For example, personal documents, official documents and media documents can be a good source for data (Bryman, 2001). In a research study related to e-Business security many documents such as an e-Business organisation's documents (e.g. security policy, employee handbook and company e-Business strategy) as well as government documents (such as e-Business strategy at the country level, ICT policy and e-Commerce act) could provide useful information related to the topic under investigation. Yin (2003) argued that documents must be used carefully and should not be accepted as completely accurate evidence. Instead, they should be used to support and enhance evidence from other sources.

Physical artifacts: many physical artifacts such as technological tools or instruments can be collected or observed as evidence in the study (Yin, 2003). For the purpose of this case study many physical artifacts can be considered as potential sources of evidence that increase our understanding of e-Business security. For example, observing e-Commerce

websites in the study environment and investigating their technical security mechanisms can provide the researcher with additional information about how security is addressed in these companies.

For the purpose of this study, semi-structured interview was the primary data collection technique. However, it was triangulated with multiple sources of evidence including document review and physical artifact review which were used as corroboratory techniques along with primary data collection techniques. Details of the data collection procedure in each unit of analysis are provided below:

- **First Unit of Analysis**: Different data sources were consulted in this unit. For instance, providers' websites provided the researcher with valuable information especially about their provenance, products, services and clients. Other data sources included annual reports and regional online business news that provided information about their projects, new products and initiatives. However, semi-structured interviews were the primary source of data. First, the providers were contacted and given an overview of the study; this was followed by an appointment with a key person from each site. To ensure a systematic way of collecting the data, a topic guide was created and followed during the interview (Arthur & Nazroo, 2003) and to get the most from these semi-structured interviews, the researcher followed the interview protocol suggested by Legard et al. (2003). Semi-structured interviews based on the topic guide were conducted involving open-ended questions covering all the overarching topics related to the study research question. Interviews were digitally recorded and transferred onto computer in order to be transcribed and prepared for the qualitative analysis stage.
- **Second Unit of Analysis**: Multiple data sources were used in the second unit of analysis in order to explore security with e-Business organisation. The primary data source was semi-structured interviews, however, other data sources, as shown in Table 3.3, were triangulated with the primary one; these included documents review and artefacts review. These secondary data sources helped to enrich the researcher's insight into the problem situation and validated some of the primary data source evidences. Semi-structured interviews allowed exploring perceptions regarding information security as part of organisational culture. In order to explore the e-

Business security in the chosen unit of analysis, individuals from different levels of the organisation (top management, middle management and employees) were interviewed. To ensure a systematic way of conducting the interview, a semi-structured interview was designed to have general themes, targeted issues and specific questions that aimed to reveal the participants' perceptions towards e-Business security. The questions were open-ended, providing the interviewees with a fair amount of freedom to answer. To ensure that the questions were not threatening, and to assist the interviewees in warming up, the themes/questions were arranged to start from some general and simple questions and then proceed to deeper ones. The interviewer was free to probe for more information and to pursue unforeseen issues. Table 3.3 shows the various data sources that were used in the second unit of analysis. The first three sources where simply used to orientate the researcher about the organisation and therefore provide better understanding for the primary data collection method namely the semi-structured interviews. The researcher conducted these interviews on-site, thus providing the opportunity for several meetings and collecting any document that provide him with information about e-Business security in the context of the study.

Table 3.3: Data sources in the second unit of analysis.

Source of Evidence	Description
Documentation	- The company annual reports over the period 2003-2007. - Regional and local online news papers.
Physical Artifacts	- The company Internet booking Engine. - The company website. - The fraud monitoring system and other internal systems.
Meetings	- Initial formal meeting with key participants followed by informal meeting (conversations) with group leaders, systems administrators provide overall understanding of the company's operational environment.
The above sources also provided invaluable inputs to the primary data collection method and allowed a deeper investigation.	
Semi-structured Interviews	- The primary data collection method. - A total of 28 participants were interviewed.

- **Third Unit of Analysis:** The primary method of data collection was semi-structured interviews. The purpose of the interviews was to explore customers' attitudes, education, awareness and expectations regarding information security in

an e-Business environment. In order to explore customer security culture and how it affects e-Business security, a sample of Jordanian citizens was interviewed. Interviews were face-to-face and took 20-30 minutes. These were digitally recorded and transferred onto personal computer in order to be transcribed and prepared for analysis.

- **Fourth Unit of Analysis:** In contrast to the previous units of analysis, document review was the primary data collection method and source of evidence that was used to analyse the government role toward e-Business security. Documents used in this of unit of analysis are shown in Table 3.4. This source of data was chosen for the following reasons:
  1. Availability: These documents are available for the public and can easily be retrieved from several government portals. Also, this make them stable and they can be reviewed repeatedly.
  2. Unobtrusive: These documents were not produced as a result of this case study and do not reflect individual officials' perspectives, but the government perception as a whole.
  3. Broad coverage: These documents cover a long span of time and many events which could provide a deeper insight into the government role in the study context.

Table 3.4: Official document reviewed in the fourth unit of analysis.

Document title	Brief description
Electronic Transaction Law No. 85 of 2001	A temporary law introduced to facilitate e-transactions without affecting the existent laws and regulations
Economic & Social Commission for Western Asia (ESCWA)'s reports 2007-2009	A set of United Nations reports outlining the progress of western Asian countries, including Jordan, toward an information society.
National E-Commerce Strategy 2008-2012	The government's plan for developing and increasing e-Commerce adoption in the country. Approved by the Prime Minister in September 2008.
Statement of Government Policy 2007 on Information and Communication Technology and Postal sectors	Replaced the government's 2003 policy to meet the rapid technological changes the country is undergoing.

In addition to the above reasons, this choice was due to the fact that the planned semi-structured interviews with a number of government representatives did not take place as

expected. Although the researcher has visited a number of governmental sites, including the Ministry of Information and Communication Technology (MoICT), the Telecommunication Regulatory Commission (TRC), the Jordan Information Technology Association (Int@j) and the special cybercrime section at the criminal investigation department to conduct the scheduled interviews, participants were not cooperative. They tended to give very brief responses and refused to have their interviews digitally recorded. However, these visits gave the researcher the chance to make some useful field notes and aided his understanding of the whole situation.

Following Yin's (2003) recommendation, each unit of analysis has its own case study protocol. According to Yin (2003), a case study protocol is a major way of increasing the reliability of case study research. This protocol defines the procedures and general rules that are intended to guide the research in carrying out data collection from each of the units of analysis. The protocol covers the following: the research question that the particular case study tries to answer; the theoretical background and framework that will help in answering the case study research question; data collection procedures; and the set of questions/themes that the case study will explore in order to answer the case study research question. Different parts of the protocol used have already been explained in the previous research design and the topic guide used in each unit of analysis is presented in Appendix A. Finally, the particular approach for analysing data collected during fieldwork is explained in the next section.

3.6.3 Inductive coding Process and thematic framework analysis

This study follows the guidelines of the general inductive approach for analysing qualitative data. This approach allows research findings to emerge from the recurrent, dominant or significant themes inherent in raw data (Thomas, 2006). It is based on inductive analysis, which has been defined as "approaches that primarily use detailed readings of raw data to derive concepts, themes, or a model through interpretations made from the raw data by an evaluator or researcher" (Thomas, 2006, p. 238). Basically, it is a five step inductive coding process (see Figure 3.3).

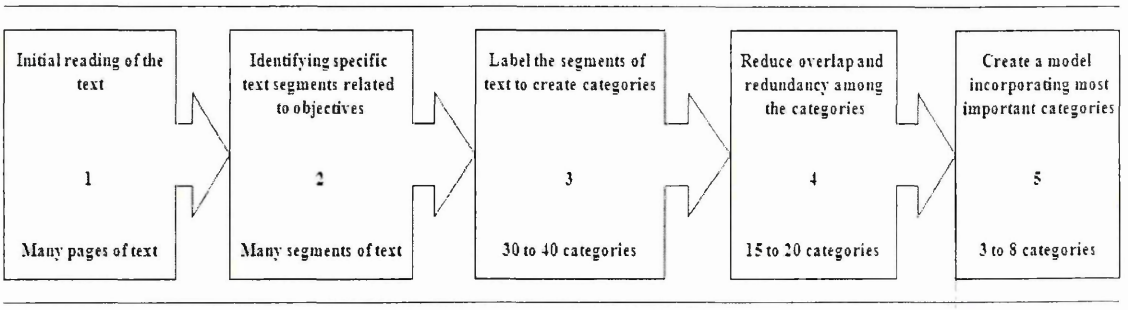

Figure 3.3: Inductive coding process adopted from Creswell (2002, p. 266, Figure 9.4).

These steps seem to be fundamental in most qualitative analysis approaches. However, some variations might be found. The process starts with an initial reading of the raw data. The first step involves several readings until the researcher feels that he has become familiar with the text. At the second step, the researcher identifies specific segments from the text; these typically depict actions, events, concepts, attitudes or behaviours that are potentially relevant to the study. At this level the coding process tends to be open and at a high level, which is why a large number of categories (usually from 30 to 40) are expected to be obtained. In the third step, each text segment identified in the previous step is labelled by giving it a category name. In the fourth step, categories are reorganised to main categories and subcategories and any repetition is removed, thereby reducing the number of categories. After this step coding tends to be more focused and selective. The researcher will start to look for the most relevant and significant categories or themes that could help him to answer the study research question. Using these categories, the researcher can create a model which shows the links between these categories and the research problem. It is worth noting that this process is not linear as shown, but in practice, involves a number of iterations and continued revision and refinement of the categories.

Unfortunately, the general inductive approach does not provide a detailed technical procedure for carrying out qualitative analysis. Therefore, the researcher has employed framework analysis technique which fulfils the general inductive approach and at the same time provides a rigorous procedure for carrying the analysis.

Thematic Framework Analysis or simply thematic analysis is one of the methods which falls under the general inductive approach for analysing qualitative data (Braun & Clarke, V. 2006; Ritchie, et al., 2003). This particular mode of analysis has been chosen for use in this study because it provides systematic and clear procedures for managing and interpreting qualitative data. As shown in the table below, this method is based on the same fundamental steps described previously in the inductive coding process. Moreover, researchers such as Ritchie at al. (2003) provide extensive technical details on how to carry out thematic analysis which is very helpful especially for researchers who are new to qualitative research.

Table 3.5: Five stages of data analysis in the framework approach, adopted from Pop et al. (2002, p. 115).

Familiarisation	Immersion in the raw data (or typically a pragmatic selection from the data) by listening to tapes, reading transcripts, studying notes and so on, in order to list key ideas and recurrent themes.
Identifying a thematic framework	Identifying all the key issues, concepts, and themes by which the data can be examined and referenced. This is carried out by drawing on a priori issues and questions derived from the aims and objectives of the study as well as issues raised by the respondents themselves and views or experiences that recur in the data. The end product of this stage is a detailed index of the data, which labels the data into manageable chunks for subsequent retrieval and exploration.
Indexing	Applying the thematic framework or index systematically to all the data in textual form by annotating the transcripts with numerical codes from the index, usually supported by short text descriptors to elaborate the index heading. Single passages of text can often encompass a large number of different themes, each of which has to be recorded, usually in the margin of the transcript.
Charting	Rearranging the data according to the appropriate part of the thematic framework to which they relate, and forming charts. For example, there is likely to be a chart for each key subject area or theme with entries for several respondents. Unlike simple cut and paste methods that group verbatim text, the charts contain distilled summaries of views and experiences. Thus the charting process involves a considerable amount of abstraction and synthesis.
Mapping and interpretation	Using the charts to define concepts, map the range and nature of phenomena, create typologies and find associations between themes with a view to providing explanations for the findings. The process of mapping and interpretation is influenced by the original research objectives as well as by the themes that have emerged from the data themselves.

This particular analysis method was developed in the UK during the 1980s for applied policy research. However, it is now widely used by qualitative researchers as it facilitates a rigorous, transparent and systemic way for concocting qualitative study (Pop et al., 2002;

Ritchie & Spencer, 1994). According to Ritchie at al. (2003) "the name 'Framework' comes from 'thematic framework' which is the central component of the method. The thematic framework is used to classify and organise data according to themes, concepts and emerging category. As such, each study has a distinct thematic framework comprising a series of main themes, subdivided by a succession of related subtopics" (p. 220). The thematic framework processes are described in detail along the first unit of analysis presented in the next chapter to give a clear description of the qualitative analysis conducted throughout the study.

3.7 Summary

A great deal of research work in the field of information systems security has been based on the positivist paradigm. Applying the reductionism concept of the positivist paradigm for information security means missing the bigger picture and thus a lack of holism, which could be one of the reasons why security is still overlooked, comes as an afterthought, or is perceived from a purely technical dimension. As a response to this, there is an increasing interest in applying interpretive-based approaches to better understand the complex and dynamic information security environment.

In this research an interpretive approach has been adopted as a means of inquiry aiming at developing a holistic understanding of e-Business security in relation to its context as well as considering all the stakeholders in the problem area. This chapter presented and justified the suitability and the need for more inductive interpretive approaches and qualitative research methods to investigate e-Business security. This methodological choice was influenced by three factors; the nature of the research problem, the researcher's theoretical lens, and the degree of uncertainty in the study environment. Toward the end, a complete research strategy for conducting the study has been presented and justified. This includes sampling, data collection and analysis procedures employed in the four units of analysis explored in this investigation. Chapters 4, 5, 6, and 7 present the findings from these four units of analysis.

Chapter 4 : Analysing the Security Role of Technology Providers

As the literature review shows, few e-Business stakeholders, apart from customers and internal organisations, are likely to be considered, and this significantly limits our understanding of the role and effect of other important stakeholders such as technology providers and governments. To fill this gap, stakeholder analysis was proposed to be used as an organising principle in this research to create a richer picture for the e-Business security environment and to consider the role of different stakeholders who may benefit from, be influenced by, or affect e-Business security in the context of the study. Therefore, the stakeholder concept has been discussed and placed within the problem domain to form a foundation for the study's conceptual framework.

This chapter presents the findings of the first unit of analysis in this research which was conducted in Jordan to explore how the security of e-Business is addressed by technology providers and what the implications of their interaction with other security stakeholders are in the problem domain. By "service providers" is meant companies that provide e-Business organisations with the required technological infrastructure which enables them to embrace e-Business. These include organisations such as software providers, hardware providers, and application developers. The terms "services providers", "technology providers" or simply "providers" will be used interchangeably in this study. Such providers have a very important role in increasing the security of the e-Business environment and will be the starting point in this investigation.

Particular procedures for conducting the study have been discussed in the previous chapter, including sampling issues, data collection procedures, and the concepts behind the analysis. In addition to this, the thematic framework and how it was used to analyse qualitative data collected in this unit of analysis will be discussed here in detail. The next section will provide background information about the providers who participated in this study.

4.1 Technology Providers' Backgrounds

Three major e-Business technology providers in Jordan - Estarta, Optimiza and STS - were investigated for the purpose of this study. The choice of these three providers was based on the reason that they are leading e-Business providers in the country; they provide most of the hardware and software required by local organisations to adopt e-Business. This section provides background information about these three providers. Their services and products can be classified as follow:

1. Third-party IT infrastructures: these include IT infrastructures such as computing and networking equipment, operating systems, and database management systems made available to the local market through partnership with international technology vendors such as HP, CISCO and IBM.

2. Third-party Off-the-shelf e-Business solutions: ready-made e-Business products which have also been bought from international third parties. These may include general e-Business solutions such as ERP and CRM applications.

3. In-house e-Business products and solutions: these include applications and solutions that the local providers have built from scratch. For instance, many financial and banking solutions have been developed by these local providers.

4. Enabling services: In addition to selling the previous products to local clients, providers provide them with a number of services that enable them to utilise e-Business. For instance, STS provide an e-payment service that can be integrated with a client's e-Business portal. Some providers make it possible for clients to host their e-Business portal completely at the provider's servers.

The following table provides a summary of the providers' provenance, core business, products, and primary clients.

Table 4.1: Technology Providers included in this study.

	P1: Estarta	P2: Optimiza	P3: STS
Provenance	• A result of a merger between two companies which have been in the market since 1991. • It is partially owned by Microsoft and Cisco Systems. • It has around 330 employees.	• In the market since 1981. • Result of a merger between numbers of local companies. • In 2006 there were about 10 companies having shares in Optimize. • The company has 400 employees.	• In the market since 1981. • In 2001, BusinessONE, the e-Business division of STS, has been established. • It has 420 employees.
Core Business	Software Development and specialised IT solutions that mainly touch on most aspects of business automation.	Technology solutions and business consulting services	Enterprise and Business solutions
Products & Services	• Mobile banking solutions. • ERP and CRM. • Document management and workflow solutions. • Business process management and integration service. • Intranet portal and content management application. • Range of services and products for transforming public sector. • Cisco based Infrastructure Solutions. • Microsoft based Infrastructure Solutions.	• E-hospital solutions. • Oracle e-Business Suite. • Enterprise Document Management Solution. • Insurance and insurance brokerage management system. • Financial accounting and analysis solution. • Call Centre solution. • Kiosk Interactive Self Service. • Workflow solutions. • Enterprise Intranet Solutions. • Enterprise Content Management (ECM). • authentication solutions through voice verification • Phone monitoring and security system. • IT infrastructures.	• Platforms & Infrastructure. • Software & Services Enterprise Portals e-Banking Solutions e-Government Solutions e-Security Solutions Third Party Products • Business Process Outsourcing. • Project Management. • Consulting. • ePayment Solutions Arcot PayONE SecureONE PAYNET. • Professional Training.
Primary Clients	• Financial Sector (Banks and other financial services). • Telecom Sector (mobile landlines operators). • Government (Public sector departments) • Commercial Sector (Merchants and private companies)	• Healthcare market. • Financial Sectors (Banking and insurance services). • Government. • Telecommunication Sector. • Enterprises.	• Government. • Financial Sector. • Educational institutes. • Telecommunication Sector. • Commercial Sector.

Estarta has been in the market since 1991, initially as two companies. As a result of a merger between these two companies, Estarta was established in 2002 with its new name. The company is partially owned by Microsoft and Cisco Systems. Currently it has around 330 employees with headquarters in Jordan and other regional offices in Saudi Arabia, UAE, Qatar and Kuwait. Estarta provides general IT solutions for its clients and one of its main focuses is e-Business applications. Prior to 2001, the company focused on off-shore projects for the US and European markets. After 2001 the company started to focus on the regional market rather than the international market. The primary target customer for Estarta is the public sector. However, other target customers include financial and telecommunication sectors.

Optimiza also is a result of a merger between a number of local companies. One of these companies is CBE which has been in the market since 1981. In 2006 there were about 10 companies having shares in Optimiza. The company has 400 employees, is based in Jordan and operates in many regional countries such as Iraq, Libya, Saudi Arabia and the Gulf region. The business focus of Optimiza can be divided into five sections; hardware, software, consultancy, training and outsourcing. It provides many banking and financial solutions and is currently engaged in many projects for automated banking, online vocational license renewal and anti-money laundering.

Specialised Technical Services (STS) has been in the market since 1981. In 2001 STS established new a unit called BusinessONE to take on the responsibility for developing e-Business applications. STS provides a range of products and services covering most aspects of information technology. It has 420 employees of whom 35 are in BusinessONE. One of the important products that STS provides for e-Business market in Jordan is PayONE which is an e-payment solution that allows organisations to integrate e-payment services with their online business. E-vouchers and prepaid cards are other payment solutions provided by STS. As a joint venture between STS and Visa Jordan Cards Services, PayNet has been implemented to be the first national e-payment gateway in Jordan. STS provides its products and services for both public and private sectors and has many projects in the region.

4.2 The Use of Framework Analysis

Data in this study has been analysed using thematic framework analysis introduced in the previous chapter. Similar procedures have been followed to interpret the study's four units of analysis. To avoid explaining this method in every unit of analysis, it will be described here in detail and in relation to the technology providers' unit of analysis. Thematic framework analysis consists of three phases: *Data management, Descriptive account and Explanatory account* (Ritchie at al, 2003). These phases in relation to this unit of analysis are discussed below.

Data management phase: After a thorough reading of qualitative data collected from the providers' interviews, the researcher created a list of themes and concepts. These initial themes were filtered according to the focus of the study and then grouped into main themes and sub-topics under each theme. After that, an index was constructed and applied to the whole data. The Data management phase provided a flexible way for grouping and managing the qualitative data. This phase has the following steps (Ritchie at al, 2003):

1. Identifying initial themes or concepts. This has been achieved by:

    a. Familiarisation with the data: the purpose of this step is to get the researcher close to the data. This was accomplished through multiple thorough readings of the data.

    b. Identifying recurring themes and ideas (perceptions, behaviours, motivations, difficulties, etc.). These were labelled as initial themes. From the providers' interviews around 40 initial themes from each interview have emerged (in total, there were 134 initial themes). Large numbers of initial themes are typical in qualitative studies. This can be explained by two reasons. First, there were recurring themes which repeated themselves in different bulks of the raw data. Second, the analysis was more open at this stage in which the researcher tried to look for all the possible ideas and themes. However, this large number of themes was reduced during the reduction and grouping process which produced sets of main themes and sub-topics.

c. Indexing: the idea of indexing is to create a numeric index for the main themes and their associated sub-topics. For instance, the main theme "1. Provider background" was assigned (1.) as index. This main theme has four sub-topics (or sub-themes) "1.1 Provenance, 1.2 Core Business, 1.3 Product & Services, and 1.4 Provider's clients". Thus, the four sub-topics have 1.1, 1.2, 1.3, and 1.4 as index numbers.

d. Grouping (reduction): all the similar and related themes were grouped together to form main themes and sub-themes.

2. Labelling or tagging the data: Applying the previous index to the data.

3. Sorting data by theme and its subtopics: creating a thematic chart for each main theme.

4. Summarising or synthesising the data: filling each thematic chart with the data related to it.

At the end of the data management phase there were 6 main themes and 32 sub-themes. These are shown in Table 4.2.

Each sub-topic has three entries: index; name/label; and initial themes in the text. For instance, the main theme ***5. E-Business Security*** has a sub-topic ***5.3. Factors affecting security P1(36,45,46) P2(6,14) P3(11,19,22,24,28)***. Thus, this sub-theme is related to the general factors affecting security and it has been indexed as the 3rd sub-theme in theme number 5. Also, it has been found to be present in data from provider 1 (P1), provider 2 (P2) and provider 3 (P3) where the entries between the brackets indicate the initial themes related to this sub-topic.

Table 4.2: Main themes emerging from the Providers' unit of analysis with their index, sub-topics and locations.

1. **Providers' Background**
   - 1.1. ***Provenance*** *P1(1,14,,12,13) P2(7,8,5) P3(6)*
   - 1.2. ***Core Business*** *P1(2,7,8,9,10,11) P2(1,2) P3(7)*
   - 1.3. ***Providers' Clients*** *P1(15) P2(5) P3(8)*
   - 1.4. ***Product and services***
2. **Availability of e-Business infrastructure**
   - 2.1. ***Availability of e-payment service*** *P3(1)*
   - 2.2. ***Availability of e-Business applications/services*** *P1(11)*
   - 2.3. ***Availability of security solutions*** *P2(6) P3(19)*
   - 2.4. ***Other***
3. **e-Business current state and future expectations**
   - 3.1. ***Providers' perspectives*** *P1(20,21) P2(3) P3(4)*
   - 3.2. ***E-Business and public sector*** *P1(21) P3(2,3)*
   - 3.3. ***E-Business and private sector*** *P1(21) P3(2,3)*
   - 3.4. ***Reasons of adoption*** *P2(4) P3(5)*
4. **Factors affecting e-Business in the study environment**
   - 4.1. ***Culture, knowledge and people related factors*** *P1(16) P2(11,12,13,15,17,20,36) P3(12,34,37)*
   - 4.2. ***Trust related factors*** *P1(18,31,51) P2(17,20,30,35) P3(35)*
   - 4.3. ***Technical factors*** *P1(19) P2(14,18)*
   - 4.4. ***Security factors*** *P1(33,45) P2(16,30) P3(18,24)*
   - 4.5. ***Other*** *P2(19) P3(11)*
5. **E-Business security**
   - 5.1. ***Security and e-Business Projects*** *P1(30,31,40) P2(23,33) P3(15,23,30,29)*
   - 5.2. ***Providers' feeling about security*** *P1(33) P2(25,26,27) P3(10,25,31)*
   - 5.3. ***Factors affecting security*** *P1(36,45,46) P2(6,14) P3(11,19,22,24,28)*
   - 5.4. ***Responsibility*** *P1(41,42,43,44) P2(31,32) P3(26,2731,39)*
   - 5.5. ***Liability*** *P1(47,48,49) P3(32)*
   - 5.6. ***Security and people*** *P2(28,30) P3(18,21)*
   - 5.7. ***Security and Business*** *P2(14,29) P3(16)*
6. **Plans, required actions and other**
   - 6.1. ***Required actions*** *P1(17,22,23,25,28,34,35,37,38,54) P2(21,24,37) P3(20,38)*
   - 6.2. ***Motivations*** *P1(24,26,27,52) P3(13,36,40)*
   - 6.3. ***Service Level Agreement SLA*** *P1(50) P2(34) P3(33)*
   - 6.4. ***Public-private sector partnership*** *P1(55) P2(38) P3(41)*

Then for each main theme and its associated sub-topics a thematic chart has been created. As shown in the first two columns in Table 4.3, each thematic chart has been filled with the data related to it as well as the line number in the original interview to provide ease of location between these chart and the original data.

Table 4.3: An example of thematic chart generated during the analysis.

Main Theme	Sub-Topic	Descriptive phase	
2. Availability of e-Business Infrastructure / Provider Name	2.3 Availability of security solutions	Element/Dimension	Category/Class
P1	As a private sector we are very advanced in things that we offer. We always comply with the industry norm of the security in most of our tenders. Most of the solutions in the market are very secure and up to the standards and best practices. (157)	compliance with security industry norms and standards	**Provider awareness regarding security standards and best practices**
P2	We are working with the Central Bank of Jordan for Anti-Money Laundering system which has been developed by Optimiza. This system will help the central bank to quickly detect and response for any suspicious transaction that may contain money laundering. (32)	Anti-money laundering systems	**Reacting to the increased demand for securing online transactions**
	Many local companies are suffering from the difficulty of getting a digital certificate to secure their websites. Still the market in this region is not well known for the international providers such as VeriSign to give them digital certificates. (66)	difficulty of getting some security solutions Unknown market	**security solutions accessibility related issues**
P3	Recognizing that we came up with a security solution for secure PIN entering over the web. This is called SecureONE and provides any online solution with a secure way for entering PIN codes and prevents keyboard and mouse sniffing. (86-89)	development of security solution for web applications	**Reacting to the increased demand for securing online transactions**

Descriptive account phase: The aim of the descriptive account phase is to understand what is happening within a single subtopic. "The main task is to display data in a way that is conceptually pure, make distinctions that are meaningful and provide content that is illuminating" (Ritchie et al., 2003, p. 237). As shown in the previous table, in this phase the researcher looked for conceptual elements and dimensions; these elements were then classified into meaningful categories. Through an eclectic blend of focusing on repeatedly recurring themes that emerged from the data as well as themes that are related to the research question, the researcher was able to refine and classify the previous themes into key elements and categories which identify the role of technology providers in an e-

Business environment. The resulting elements and categories are shown in Table 4.4. Two main categories have been defined in this phase:

1. **E-Business Stakeholders**: These represent the set of elements surrounding the service provider; these elements are located outside the provider's internal environment and they are not under his direct control and they may interact, affect or be affected by the providers. E-Business stakeholders and their interrelationships with the services providers will be discussed section 4.3.

2. **Providers' operating context**: This represents all the elements that the service provider is able to influence or control. This clearly includes the provider's provenance, products and services, and core business. Moreover, it also includes their assumptions and beliefs regarding e-Business and e-Business security. This operating context in relation to the stakeholders identified is discussed in section 4.4.

After indentifying these categories and their associated elements, boundaries of the providers' problem situation have been constructed. This point marked the start of the explanatory account phase in which the researcher explored the relationships between these categories and how they affect each other. Explaining these emerged conceptual elements in relation to the providers' role in e-Business security environment is the main task of the explanatory account phase.

Explanatory account phase: In this phase the researcher started to look for linkages between sets of phenomena and developed explanations. This was achieved by looking for patterns of association within the data and then explaining why these patterns occur. According to Ritchie et al. (2003), building explanations is usually based on two types of reasons; explicit reasons that emerge directly from the data and implicit reasons inferred by the researcher. The explanatory phase is for telling the main story that provides a clear and coherent picture for the phenomena under investigation. At the end a model showing the generated categories including all the conceptual elements and their interaction can be produced.

Table 4.4: Key elements and categories identifying providers' security role in e-Business environment.

Stakeholder	Data from P1	Data from P2	Data from P3
Clients	• Now we have project with the government to provide one of their service over the Internet. • One of our main focuses is e-Business especially in the public sector. • As a customer we have the financial services and what we call commercial sector; telecomm and private companies.	• Part of this project is to connect number of government departments. • We are working in many projects for automating some banks in Jordan.	• In 2001 we launched an e-payment initiative which originally was a tender between the Arab bank and the social security department. • Number of merchants are using it; Zain, Orange and Umneiah. • We are trying to bring some of the potential customers such as RJA and Zalatimo.
Governments	• Recently we have seen many initiatives from MoICT regarding this matter. • I believe by spreading the government e-services things will be changed. • And the government should intervene at a certain stage to regulate this.	• It gives security high priority but in our project since it is completely running over the government network there is no risk.	• As much the government puts their services over the internet as much the citizens are motivated to use the internet in their daily life activities. • Government should enact the laws and legislations that protect online customers as well as online service providers.
Customers/Citizens	• When many things become online, like bills for instance, people will be motivated to use it. • Many banks start to charge the walk in customers more than the online ones. • People still don't have the confident to deposit money using the ATM. • If people start feeling that the environment is not secure, they will not use it.	• Citizens need to go physically to the required government department. • If you talk about e-commerce and e-Business, you are targeting a wide rang of people. So, the problem related to this wide rang of people. • Any fear from the side of people regarding security will kill the business.	• The young generations are looking for such things [e-Business]. • If people find that the online service will cost them more than the normal service they will choice the normal service even if this might cost them some extra expenses such as transportation or whatever. • I think people started to have some sort of knowledge about security. So we need to focus more in security as well as spreading the knowledge about how much e-services can make life easy.
International bodies	• We always comply with the industry norm of the security in most of our tenders. • Most of the solutions in the market are very secure and up to the standards and best practices.	• Many local companies suffering from the difficulty of getting a digital certificate to secure their websites. • Still the market in this region is not well known for the international provide such as VeriSign to give them a digital certificates.	• I think the existence of some standards such as PCI which created by Visa and MasterCard compensate for the customer awareness because the vendors should follow these standards and take care of the customer information. • We are in the process of certifying our products according to the PCI standard.

Providers' operating environment	Data from P1	Data from P2	Data from P3
Provenance	• A result of a merger between two companies which have been in the market since 1991. • It is partially owned by Microsoft and Cisco Systems. • It has around 330 employees.	• In the market since 1981. • Result of a merger between numbers of local companies. • In 2006 there were about 10 companies having shares in Optimize. • The company has 400 employees.	• In the market since 1981. • In 2001, BusinessONE, the e-Business division of STS, has been established. • It has 420 employees.
Core Business	Software Development and specialized IT solutions that mainly touch on most aspects of business automation.	Technology solutions and business consulting services	Enterprise and Business solutions
Products/ Services	• Mobile banking solutions. • ERP and CRM. • Document management and workflow solutions. • Business process management and integration service. • Intranet portal and content management application. • Range of services and products for transforming public sector. • Cisco based Infrastructure Solutions. • Microsoft based Infrastructure Solutions.	• E-hospital solutions. • Oracle e-Business Suite. • Enterprise Document Management Solution. • Insurance and insurance brokerage management system. • Financial accounting and analysis solution. • Call Center solution. • Kiosk Interactive Self Service. • Workflow solutions. • Enterprise Intranet Solutions. • Enterprise Content Management (ECM). • authentication solutions through voice verification • Phone monitoring and security system. • IT infrastructures.	• Platforms & Infrastructure. • Software & Services • Enterprise Portals, e-Banking Solutions, e-Government Solutions, e-Security Solutions, Third Party Products. • Business Process Outsourcing. • Project Management. • Consulting. • ePayment Solutions Arcot, PayONE, SecureONE, PAYNET. • Professional Training.
e-Business Perceptions			
❖ **Optimistic feeling about the progress**	• It is a natural progress and a matter of time. • We are ahead of many countries.	• There are big steps in the field.	• E-Business is promising and potential. There is a good progress.
❖ **Government, Banks and human resources have strong impact on e-**	• Government initiatives are helping.	• It is in the banks more than other companies; banks are leading e-Business.	• Young educated people are the key stone for succession of e-

Business.			Business project.
❖ **Lack of e-Business Culture and Technology distrust are the main *obstacles***	• You can not talk about e-Business without the culture of e-Business. • They don't have enough trust on the technology.	• Still the culture of credit cards is not popular. • People still don't trust the internet and don't accept to put their credit cards numbers on the internet.	• Culture need to be changed. • I trust the technology, but my father doesn't.
Security Perceptions			
❖ **Appreciating Security**	• Security is important element and this increases if we talk about online services because you will be more vulnerable to the attacks.	• It is very important. Any fear from the side of people regarding security will kill the business.	• First of all security. It is very important.
❖ **Shared Responsibility toward Security**	• You cannot specify one body to be responsible for e-Business security.	• The vendors are responsible. For example, if we provide e-payment service we will be responsible for its security.	• Many entities are responsible for that.
❖ **Recognising the Impact of Security on *Business & People***	• So if people start feeling that the environment is not secure, they will not use it.	• Any fear from the side of people regarding security will kill the business.	• The product should be highly secure. If you failed once, you may loose everything.
❖ **Security is a Function of Cost and Client's Request**	• Solutions go though different number tests. And of course this is based on the customer request. • Security is a function of cost.	• You will never use a website with questions marks on its security or if you just hear that it has no security.	• It is your reputation and creates trust with your customer from one side and with the services provider from the other side.

The rest of this chapter presents the findings of this unit of analysis including explanatory accounts for the role of technology providers in the study environment and how they affect the trustworthiness of the e-Business environment through their approaches to security and interactions with other stakeholders. Section 4.3 discusses the emerged stakeholders, their interactions with and impact on technology providers. Section 4.4 discusses the providers' operating environments and their perceptions of security of e-Business environments. These findings are synthesised in the summary section and set the stage for the analysis carried out in the next chapters (5, 6 and 7).

4.3 Stakeholder Identification and Analysis

A holistic understanding of the role of technology providers in the dynamic e-Business security environment cannot be achieved without understanding their interrelationships with the diverse parties involved in an e-Business environment. Therefore, stakeholder analysis was a natural choice which fits the exploratory nature of this research. As shown in Table 4.4, several stakeholders who directly or indirectly interact with technology providers have been identified:

- **Clients**: These represent the provider's current and potential clients and may include any organisation embracing or willing to embrace e-Business activities. From the analysis, it seems that financial institutions such as banks and insurance companies, telecommunication operators, and the government represented by its public departments, are the primary clients in the study environment. Whilst some clients come from healthcare and educational sectors others come from the commercial sector, such as merchants and private companies.

- **Customers/Citizens**: These represent the body of citizens including the clients' current customers and the potential ones; they interact indirectly with the providers through their previously mentioned clients.

- **Government**: This represents the role of the state and includes all the governmental departments and regulatory bodies which may have direct of indirect impact on e-Business in the country. The Ministry of ICT and the Telecommunication Regulatory Commission (TRC) are examples of such government departments in this study.

- **International bodies**: These represent external bodies which impose provisions on the local technology providers or their clients in order to utilise some aspects of e-Business. For instance, the major credit card companies such as Visa and MasterCard have implemented a Payment Card Industry (PCI) standard and require any application developer, bank or business organisation to comply with PCI standard in order to be able to use their cards in any electronic transactions. Other examples of such external organisations are the certificates authorities or trusted third parties who provide digital certificates which are an important component for implementing secure e-Business portals.

Table 4.5: Providers' and stakeholders' interactions and their impact.

Stakeholder	Thematic Observations	Impact on Technology Provider
Clients	Increasing demands for e-payment services. Increasing demands for automating financial services. Emergence of internet banking notion. Increasing demands for automating public services.	Motivating providers to focus on developing e-Business applications with more emphasis on financial and public sectors.
	Requesting features other than security.	Providing basic security features based on ad-hoc approaches
	Increasing demands for up-to-date e-Business applications and infrastructure.	Partnerships with international vendors such as DELL, IBM and Cisco to fulfil the market needs.
	Increasing demands for securing e-Business transactions. Absence of specialised security vendors. Absence of real efforts to market e-Business and security of e-Business.	Developing some sort of ad-hoc security solutions in addition to providing off-the-shelf products to fulfil security needs. No clear strategies for e-Business security.
Governments	Launching number of initiatives to increase ICT diffusion.	Creates more business opportunities for the providers and motivates them to invest in e-Business and ICT fields.
	Lack of clear and comprehensive e-Business regulations.	Lack of guidance and reference.
	Absence of real partnership with private sector.	No channel for communicating suggestions or knowledge exchange
Customers/ Citizens	Lack of e-Business culture in people daily activities. Low level of credit cards penetration. Internet related technology distrust.	Force providers to look for alternative ways and options to encouraging people to use e-Business services. For example, introducing repaid cards, e-vouchers, cash on delivery... etc.
	Indication of increasing awareness, however, awareness level is still low.	Force providers to pay more attention to security.
International bodies	Compliance requirements for standards such as PCI standard.	Increasing providers' security awareness Motivating them to follow good practices as preface for the compliance.
	Difficulties in getting security components from international providers such as VeriSign.	Hinder e-Business deployment

A bidirectional interaction exists between the providers and these stakeholders. This interaction can be explicit in the form of exchanging products, services, information and knowledge. However, the interaction can be implicit and influence a particular provider's perception or behaviour. For example, the government may introduce a new rule to protect citizens' privacy. Such a rule would influence the clients who may request additional privacy controls from their providers.

From the providers' analysis it has been possible to investigate the impact of providers' interactions with the stakeholders in their security role in an e-Business context. This is presented in the following subsections. The interpretations are based on thematic observations (see Table 4.5) that have been generated from the thematic framework analysis presented above.

4.3.1 Impact of clients' requirements

From the analysis it was clear that many clients - mainly, governmental public departments, financial institutes and telecommunication companies – have become interested in embracing e-Business and enjoying its claimed benefits. These increased demands have had an impact on technology providers. They motivated them to focus on developing e-Business applications and services as well as providing the necessary technical infrastructure that allows clients to utilise e-Business. There was a clear focus on developing e-Business solutions with more emphasis on financial and public sectors because the majority of the demands were from these two sectors.

Features such as performance, functionality and ease of use have been recognised by the clients at the expense of security. Consequently, providers focused on these features rather than security and as a result they provided only basic security with their products, which in most cases involved ad-hoc approaches. In addition to the previous observations, there was a notable increase in the number of organisations adopting e-Business in the country (AMEinfor, 2007; Stensgaard, 2006). Many clients and their customers have become more familiar with e-Business applications. Applications such as internet banking, e-billing and e-ticketing have become popular in many sectors. Thus, the demands for new and up-to-date e-Business products and services have increased. Moreover, when e-Business started to involve complete financial transactions, security started to get more much attention. These new demands created a competition between technology providers in order to meet

the market needs. Most of the local providers depend on partnerships with international vendors such as DELL, Cisco and IBM to fulfil these increasing demands. In addition to partnerships with international security vendors to supply the market with off-the-shelf security solutions, providers try to develop some sort of security products to meet their clients' needs.

When asked how they ensure security in their projects and products, there was no common answer. Some providers responded by saying that the product goes through a number of tests to make sure it is secure, others said that they ensure security by following some security standards, while some did not give a clear answer. Although some providers believe security should be a built-in and integrated part of e-Business solutions, other providers mentioned some cases in which security was added later, after a solution had been experienced by many customers. Thus, the *after deployment breaches* were one of their techniques for improving security. Moreover, the role of the security expert/engineer was not defined under their organisational structures. There were no security engineers participating in e-Business projects. No evidence was found to indicate that providers follow systematic methodologies or procedures for ensuring security in e-Business projects they undertake. The problem in such e-Business security implementations is that the components of e-Business infrastructure are looked at individually and separately from security purposes, which makes security solutions ad-hoc and component driven (Otuteye, 2003). The existence of such security solutions may give the client a false feeling of security, especially if they are not built and erected based on a systematic approach to information security (Siponen, 2005).

4.3.2 Impact of absence of clear guidance and regulations from the government

Providers mentioned a number of initiatives that the government has launched to promote ICT and encourage different private and public sectors to adopt electronic means for doing business[3]. These initiatives are considered by them as a positive step towards an e-Business culture. In fact, these government initiatives have an impact on local technology providers because they have created more business opportunities for the providers and encourage them to increase their focus on the e-Business field to provide all the necessary infrastructures required by both public and private sectors. This is evident in the large

[3] see MoICT website for list of ICT initiatives: http://www.moict.gov.jo/MoICT/MoICT_Initiative.aspx

number of e-Business products and services which target such government initiatives. Yet the government is not meeting the expectations of providers, who have argued that the government should participate in setting standards and regulations for e-Business in the country. They have stressed that the government should take an active role in protecting online customers. Additionally, they believe that the government can help in making important e-Business security components such as PKI and smartcards available in the market.

It is clear that these government initiatives were not combined with clear guidance and regulations which would cultivate security and force the providers to follow a rigorous approach in developing and deploying their products and services. Despite the debate about whether such regulations could help in increasing security or not (Schneier, 2006), the researcher believes the existence of these regulations would help in creating a common framework to provide adequate levels of security assurance in e-Business projects in the country instead of leaving the whole matter to the judgment of individual providers.

4.3.3 Impact of absence of real collaboration with the government

Lack of communication is another aspect which was uncovered during the exploration of interaction between the government and the technology providers. Despite the fact that the government keeps promoting the concept of public and private sector partnership (MENAFN, 2008) e-Business seems to have benefited less from this. Providers argued that there was no mechanism for suggesting things to the government. Arguably, the absence of real partnership between the government and the private sector in general and e-Business providers in particular closes the door for communicating suggestions and knowledge exchange. The government seems remote from the providers who have more skills and deeper knowledge in the e-Business field. Therefore, the existence of such channels could benefit both sides. The government could play a major role in establishing communication channels between all the parties interested in e-Business security. In fact this is the case in many developed countries. For instance, a number of the US government agencies organise software workshops where vendors, academics and customers discuss better software security practices (Davidson, 2008).

4.3.4 Impact of citizens' lack of e-Business culture and distrust of technology

Clients' customers indirectly interact and influence technology providers because clients fulfil many of their customers' demands and expectations through requesting new services and products from the technology providers. From the providers' perspectives, Jordanian citizens still do not have an e-Business culture and the majority have never engaged in real e-Business transactions. This lack of e-Business culture was attributed to different reasons, such as lack of computer literacy, low levels of internet penetration, and complete absence of e-Business awareness. Providers argued that the lack of an e-Business culture creates distrust about internet-related technology especially for financial transactions, as in e-Business applications. To overcome this issue, they started to look for alternative ways of getting more customers into the digital environment. For instance, prepaid cards, e-vouchers and cash on delivery have been introduced for use by customers who do not have credit cards or who are not comfortable using their credit cards over the internet. While these solutions might help in increasing the adoption of e-Business in the country, they do not overcome the issues of customers' knowledge and awareness of e-Business security which underlie customers' distrust of technology. On the other hand, service providers believe that if customers start to have more security-related knowledge, this will provide a better understanding of security and perhaps greater assurance, and thereby secure their products and services. They feel that customers' security awareness can positively affect the security of e-Business products and services because this will force them to pay more attention to security in their products and services so that customers can use them with greater confidence.

4.3.5 Pressure of standards compliance

Another factor which influenced the providers' role toward security came from external stakeholders, represented by international organisations and accreditation bodies. These organisations have developed standards and best practices to provide security assurance in e-Business applications. Compliance with such standards is either compulsory or strongly recommended as these organisations have developed strong reputations and commitment to their customers. Thus, this directly influences the trustworthiness of e-Business applications. Providers pointed out that the existence of such standards could compensate for the customers' lack of awareness since they ensure some levels of security. However,

these standards still do not have a significant effect because there are no regulations to enforce compliance with such standards and local customers are not yet familiar with them. Only one of the providers stated that the company is in the process of complying with the Payment Cards Industry (PCI) standard developed by Visa and MasterCard because the standard mandates clients and service providers to meet particular security requirements when they process cardholders' information. Another external impact came from international certificate authorities such as VeriSign. Providers claimed that applications to get Digital Certificates (DCs) from such international Trusted Third Parties (TTPs) are often declined and this hinders the deployment of e-Business in the country. They argued that these TTPs are very concerned about their reputation and are not willing to take the risk of providing DCs to clients in an "unknown" market.

The previous defined stakeholders - clients, customers, government, and international bodies - have significant impact on how the local technology providers handle e-Business security in the study environment. In the light of this stakeholder analysis, and to get more insight into the providers' security role, the next section will identify their perceptions of e-Business security in their operating environment.

4.4 Providers' operating environment and their perceptions of e-Business Security

Similar to the process followed in section 4.3, the researcher looked at a number of thematic observations in order to understand how providers perceive security and what really affects their perceptions. He started by exploring their perceptions regarding key issues (e-Business growth, enablers and barriers) in the environment in which they operate and then moved on to their perceptions of e-Business security. Four key perceptions emerged regarding e-Business security which will be discussed in section 4.4.2. Table 4.6 provides a summary of providers' perceptions of e-Business and security as well as the impact of these perceptions.

Table 4.6: Providers' perceptions and their impact on e-Business and security.

Operating Environment	Thematic Observations	Impact on technology Providers
Perceptions Toward e-Business		
Growth of e-Business (Natural progress)	This perception is a result of the increasing number of clients embracing e-Business in the country in addition to the government initiatives to create e-society.	Optimistic feeling about the progress on e-business in Jordan. Motivates providers to invest in e-Business.
e-Business enablers (Government, Banks and Skilled People have strong impact on e-Business)	This perception is a result of the following: recognising the traditional role of the government, e-government project, notable increase in automation of financial services and e-banking and the high percentage of well-educated people.	Focus on developing e-Business applications particularly for the government and financial sectors.
e-Business Barriers (Lack of e-Business Culture and Technology distrust are the main obstacles)	This perception is a result of the following: percentage of citizens who perform real e-business transaction, low level of credit cards penetration and citizens' lack of e-Business knowledge.	Providing alternative solutions and options to overcome some of the cultural and trust issues.
General Perception Toward Security		
Appreciating Security	Despite this appreciation there is no evidence proof that e-Business security is perceived from any point of view other that the technical one.	Increasing the interest in developing and providing security technical measures.
Shared Responsibility toward Security	No clear definition for these responsibilities. No obligation or enforcement.	Self-judgement and the risk of waiting for others to fulfil their responsibilities first.
Recognising the Impact of Security on Business & People	No systematic approach for addressing this impact	Adopting ad-hoc and technical approach for addressing e-Business security.
Security is a Function of Cost and Client's Request	Client is usually depends on the vendor to provide security.	Provider is only committed to provide basic security.

4.4.1 Perceptions of e-Business in the study environment

Providers' perceptions which emerged in this study were related to fundamental issues in e-Business diffusion. These e-Business issues have been discussed in the literature in terms of stage of growth, enablers of and barriers to e-Business (Daniel et al., 2002; Zhu et al., 2003 and Kshetri, 2007). The revealed perceptions were influenced by the stakeholders identified previously and have several impacts as shown in table 4.5. These perceptions and their implications are discussed below.

Growth of e-Business

Technology providers described the current diffusion of e-Business in the country as a natural progression and as a matter of time. According to them, there are big steps in this

direction, which they considered promising and as having potential. Compared to other countries in the region, they considered Jordan ahead of many countries and that e-Business has a good competitive position in the region. In addition to that, they felt awareness about the benefits of e-Business is increasing and this will positively affect e-Business diffusion. This optimistic feeling seems to be a result of the increasing number of clients embracing e-Business in the country and the government initiatives to promote ICT. This has created more business opportunities for them and encouraged them to invest more in the e-Business field, which is evident in the wide range of e-Business products and services that they supply the market with. The maturity of e-Business can be described using e-Business stages of growth models suggested by number of researchers (see for example Earl, 2000). These models suggest a number of stages that an organisation is likely to experience during the adoption process. Prananto et al. (2001) argued that most of these stages of growth models define three to four stages: "with organisations moving from no presence on the Web, through a static, informational presence ultimately to full-blown electronic business-to-business and business-to-consumer trading over the Internet" (p. 1255). This study's findings and those of other studies (Al-Qirim, N. 2007) indicate that e-Business in Jordan is still in its early stages and is not widespread in the country; the majority of the online population (from private and public organisations) has informational presence with few organisations which have introduced the B2C mode in their businesses. According to Earl (2000), such a situation can be explained by the classical theory of diffusion of innovation proposed by Rogers (1962) and this confirms the providers' point of view that e-Business diffusion in the country is a matter of time.

E-Business enablers

Three entities were considered by the providers to have a significant impact on e-Business diffusion in the country: government, banks, and skilled people. Providers appreciated the government's initiatives for reducing internet prices and increasing technology penetration. This perception of the government could be attributed to recognising the traditional role of the government and to the growing number of government ICT initiatives which have created more business opportunities for them. The impact of these initiatives is clear in the increasing number of providers' products and services which targeted government public departments. In addition to the government, banks were considered by the providers to be the leaders of e-Business initiatives because they like to have their business automated,

accurate, and without the manual intervention that can slow down or tamper with their business. This explains why providers have a wide range of banking and financial solutions. The last e-Business enabler mentioned by the providers was skilled people and, as they put it, young educated people are the keystone for the success of e-Business projects in the country: this seems a result of the high percentage of well-educated people in the country. These findings conform with many studies which investigated e-Business enablers. Many entities have been considered to have significant influence on e-Business adoption. Papazafeiropoulou et al. (2001) argued that governments and policy makers have an important role in improving e-Business adoption. Wenninger (2000) discussed the role of banks in the e-commerce age and how they can act as e-commerce facilitators. Other researchers emphasised other factors enabling e-Business, such as technological infrastructure, skills and knowledge (Weill & Vitale, 2002).

E-Business barriers

Providers highlighted that the lack of an e-Business culture is a major obstacle for e-Business diffusion in the country. They gave many examples to demonstrate the effect of the absence of an e-Business culture. For instance, the majority of people do not have credit cards and only a small percentage of the credit card holders use their cards over the internet. Moreover, providers stressed that engagement in e-Business activities such as e-commerce and internet banking is only notable among the younger generation in the country. In addition to the lack of e-Business culture in peoples' daily activities, they argued that people do not have enough trust in internet-related technologies. Consequently, providers look for alternative solutions to overcome the culture and trust issues. For example they have introduced cash-on-delivery, prepaid cards and e-vouchers. As discussed in section 4.3, these solutions did not address the real issues which relate to people's knowledge and awareness of e-Business. Arguably, this distrust does not foster e-Business and therefore negatively impacts on its diffusion in such a country (Aljifri, 2003). Such cultural issues were discussed by Yasin & Yavas (2007) who suggested that both the government and the private sector should contribute in creating e-Business culture.

4.4.2 Perceptions of e-Business security

Investigating the providers' perceptions of security aided better understanding of their particular approaches to address security and what really affected these approaches. Four

security related themes emerged from the data; appreciation of security, shared responsibility, impact on business and people, and cost. These themes depict the providers' perceptions towards e-Business security and influence their approaches to addressing it in the study environment. However, the study revealed that these perceptions are highly affected by the interaction with the stakeholders identified previously. These perceptions and the various factors affecting them are discussed below.

General appreciation of security

Security in general seemed to be appreciated by the providers. Most of them felt that security is very important, especially in the web environment which is utilised by e-Business applications. They believed that utilising the internet rendered business more vulnerable to attacks than any time before. Therefore, they argued that extra attention needs to be paid to security. Despite this perception of security, there is no strong evidence that they perceive e-Business security from any viewpoint other than a technical one. This technical orientation is regarded by many researchers as contributing to an increase in the security problem that we are facing today (Flechais & Sasse, 2009; Zurko & Simon, 1996). The providers' appreciation of security combined with the technical orientation may explain why the providers focused on providing the market with security solutions with extremely technical measures such as firewalls, anti-viruses and encryption mechanisms. Such technical solutions are not a silver bullet and have their own inherited shortcomings and design flaws (Geer, 2004) which make the situation worse.

Shared responsibility toward security

There was consensus between the providers that responsibility toward e-Business security is a shared responsibility. They believed that one body cannot be responsible for the security of e-Business. Instead, they believed that many entities should share this responsibility. They argued that e-Business organisations (clients), technology providers, business partners, government and customers share this responsibility. From the researcher's perspective, it is important that technology providers recognise shared responsibility in e-Business security, an issue which has been raised recently by industrial leaders and international commissions (Ballmer, 2004; Reding, 2007). However, the lack of clear definition for each stakeholder's responsibility and the absence of regulations which enforce it leave the responsibility to the providers' own judgement. Moreover, and in such a

situation, this perception could raise the risk of waiting for the other parties to fulfil their responsibilities first.

Recognising the Impact of Security on Business & People

The impact of security on business as well as people was clearly recognised by the providers. Security was regarded as an important factor for creating trust and reputation. They claimed that security increases their customers' confidence in e-Business products and services. Providers argued that e-Business transactions need to be secure and people should be convinced that their transactions are secure, or else they will not use e-Business. While some providers believed that products should be very secure and there should not be any breaches, others believed that nothing is 100% secure. Yet providers did not show any systematic approach for addressing this impact. For instance, marketing in general seems to be the last thing they thought about. When it comes to marketing security, nothing seems to be offered. They mentioned that the whole budget goes to the development stage and at the end of the project they do not find money for marketing the products, which is considered costly. Arguably, marketing security could play an important role in the e-Business security environment. It could contribute to raise customers' security awareness, create a sort of competitive advantage and encouragement to utilise e-Business. Marketing security has been highlighted by Suh & Han (2003), who argue that customers can only recognise the strength of security of a site indirectly through advertisements and publicised information.

Security is a Function of Cost and Client's Request

Security was considered by the providers as an extra cost which they tried to minimise or avoid. Therefore, they were willing to provide only basic security measures such as simple authentication and authorisation mechanisms with their e-Business products and services. They argued that any additional security measures should be based on the client's request. In this way they can avoid any extra cost since the client will be charged for these extra requirements. Unfortunately, it is not always the case that the clients are fully aware of the security requirements of e-Business applications. For instance, many small companies who wish to benefit from the online environment lack knowledge of security and the budgets necessary to cover its requirements (Wymer & Regan 2005). Therefore, clients are likely to depend on the providers who are supposed to know the detail of their products.

4.5. Summary of the Provider's Security Role and the Way Forward

All the previous findings will be synthesised in this section in order to create a richer picture for the current role of the technology providers in security in an e-Business environment. To achieve this, the researcher explored how they addressed security and what really influenced their approaches to ensure security. Using stakeholder analysis it was possible to identify the different stakeholders who, through their interactions with the providers, were found to have direct impact on how the providers perceived and dealt with e-Business security. The study findings have been incorporated in a conceptual framework (See Figure 4.1) which represents the key themes which have been found fundamental to understanding how providers addressed e-Business security.

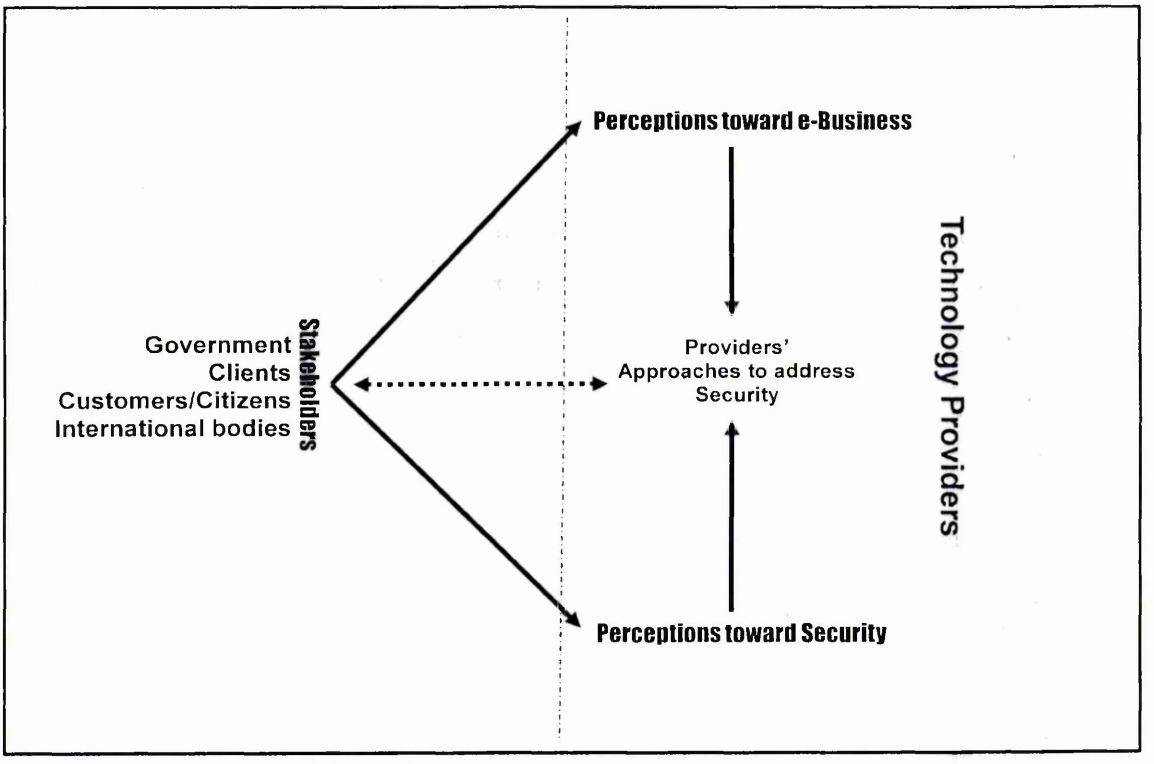

Figure 4.1: Factors affecting the security role of technology providers in e-Business environment.

Their ways to address security of e-Business were based on providing their clients with all the technical solutions that they believed would ensure it. These solutions are either off-the-shelf products, such as firewalls and anti-viruses from international vendors, or basic modules integrated with their products and services to provide authentication and/or authorisation security services. These give the indication that security is treated as a product

not as a process which needs to be ensured and integrated everywhere. Security was not systematically managed and this is evident in the e-Business projects which did not involve information security risk management processes to identify threats, vulnerabilities and mitigations. Moreover, the role of the security engineer was missing in these projects, increasing the chance that security would be overlooked and come as an afterthought.

From investigating interactions with diverse stakeholders, it is clear how much they affect the providers' perceptions about e-Business. On one hand, some stakeholders had a significant role in motivating providers to develop and invest more in e-Business. For instance, government initiatives to increase e-Business adoption and the increasing number of clients adopting e-Business made them feel optimistic about the future of e-business in the country and motivated them to supply the market with many e-Business products and services. On the other hand, stakeholders had a negative impact on the providers' security perceptions. For instance, the absence of government regulations, clients' lack of security knowledge, and customers' lack of security awareness fostered non-systematic technical orientation of the technology providers to deal with security of e-Business.

Despite the recognition of the importance of security and its effect on business and people, these perceptions did not encourage technology providers to look at security from any perspective other than a technical one. This could be explained by two reasons. First, the stakeholders' current interests are not driving toward a comprehensive way of addressing e-Business security. For instance, e-Business diffusion and providing its necessary infrastructures seem to have higher priority on the government ICT agenda and as a result there are no regulations to force providers to focus more on security. Moreover, clients want to get the most from adopting e-Business as soon as possible, therefore, features such as functionality and ease of use are recognised at the expense of security. Second, the providers try to keep the cost associated with providing their clients with security to the minimum. To achieve this, they provide some basic security features and off-the-shelf security products that clients can buy separately. Any additional advance security requirements are left to the client who will be charged for them. For the same reason marketing and promoting security are completely ignored as they are considered costly.

Based on the above discussion, technology providers' approaches for addressing e-Business security can be described using one or more of the following:

- Ad-hoc: Not based on a well defined methodology for addressing the real risks involved in e-Business environment.
- Purely Technical: Based solely on providing technical solutions without considering the social environments where these solutions are going to be used.
- Afterthought: In some cases security is added later, after the solution is experienced by end users and vulnerabilities are discovered.

These approaches, which do not recognise security as a multidimensional and continuous process, can negatively affect the security of e-Business environments and therefore, impact on their trustworthiness, which can only be achieved through addressing the long-term security needs of e-Business stakeholders. They only focus on short-term concerns of the stakeholders and do not contribute to raising the security awareness and knowledge which could have a positive impact on security.

While this analysis explored and explained how the security role of the technology providers affects and is affected by the e-Business environment in the context of this study, its findings highlighted some aspects of other stakeholders which need further investigation in order to fully understand their influence on the security of e-Business. Security aspects of these emerged stakeholders (e-Business organisations, customers and government) are analysed in the following chapters (5, 6 and 7).

Chapter 5 : Analysing Security within e-Business Organisations

This chapter presents the findings of a case study which was conducted in an e-Business organisation, representing the second unit of analysis in this research.

An e-Business organisation represents by itself a complex socio-technical subsystem which has management, employees, information, services and infrastructure; these represent the internal stakeholders of e-Business security and have dynamic interactions with each other as well as with the environment. Shortcomings in any one of them might create security breaches that could affect the other components leading to compromise of the whole e-Business organisation. Therefore, understanding the security perceptions of the social components (management and employees) as well as the security requirements of the technical components (information, service and infrastructure) and how they affect each other is a significant step in forming a holistic understanding of e-Business security. Therefore, the research question that this unit of analysis seeks to answer in this organisation-level case study is:

How is security perceived in the context of e-Business organisations in the study environment? And what are the implications of this perception?

To fulfill the quest of this research and to follow systematic investigation, this research question is divided into set of related sub-questions, whereby the answer to each question leads to the following one and sets the stage for further investigation, ultimately leading to comprehensive understanding of the problem situation. These sub-questions are formalised as follow:

1. How do e-Business activities emerge in the context of the chosen unit analysis? (Sections 5.1 and its subsections cover this question).
2. What are the various groups of stakeholders involved in e-Business security? (Section 5.2 covers this question by providing detailed analysis of the operating environment and various stakeholders involved in it).

3. How do internal stakeholders perceive and interact with e-Business security? (Section 5.3 presents the themes which emerged related to the stakeholders' security perceptions. Sections 5.4 to 5.7 provide a detailed analysis of each of the previously identified internal stakeholders in relation to e-Business security.)

Findings from the above analysis were synthesised in order to provide answers to the following questions:

1. How do internal stakeholders handle e-Business security? (Section 5.8 discusses this issue)
2. What are the socio-technical factors which affect security in the context of e-Business organisation? (Section 5.9 discusses these factors)

An airline company which undertook major transformations to adopt e-Business has been chosen as the second unit of analysis in research. Sampling issues and data collection procedures related to this unit of analysis have been discussed previously in the research design presented in Chapter 3. The next section provides background information about the selected unit of analysis.

5.1 Unit of analysis background

The Royal Jordanian airline (RJ) was established in 1963 as a national carrier with a vision to connect Jordan with the world. The company went through privatization in 2007 when ownership was transferred to the private sector to become the first privatised Arab airline (Arab Air Carriers Organisation, 2009). The company has headquarters in Amman and a network covering more than 50 destinations around the world. In the last six years there has been a notable increase in adoption of information and communication systems in RJ's day-to-day business activities. After the invitation to join the oneworld alliance in 2005 (RJ's annual report, 2005), RJ undertook a number of projects to develop its infrastructure and adopt e-Business applications and as a result it is ranked by the International Air Transport Association (IATA) as an advanced e-commerce airline (AMEinfo, 2007). In 2007 the company officially joined oneworld after fulfilling the technological requirements to be part of the alliance. In the same year the company won the golden award for the best website of an Arab carrier (AMEinfo, 2007).

5.1.1 Early days of e-Business in RJ

According to company records and meetings with senior IT staff, the use of electronic business in the company can be traced back to the 1970s when the IT department started to automate some of the company's services. The company owned two IBM mainframe computers; one was installed as a production machine and the other was a backup machine. The production mainframe hosted all company critical applications, such as the financial system, cargo system, asset management system, personnel application, and insurance application. When the the oneworld alliance came into the picture, the mainframe could not meet the high speed and instant transactions required by the alliance (RJ's annual report, 2005). Therefore, the company moved into the client-server architecture which provided an efficient way to communicate with other airline companies within the alliance. The company obtained HP servers with Linux operating system and started by replacing the old financial systems with a new one brought from Lufthansa as a first step to replacing all the other old systems and switching off the mainframe completely. During 2002-2004 RJ worked on developing its communication infrastructure and increasing its network speed. To improve internal communication, an e-mail system was implemented and intranet made available to the RJ's employees to access information related to their employment, such as salaries, vacations schedule and access to free tickets (RJ's annual report, 2005).

5.1.2 The emergence of B2B and B2C e-Business in RJ

Analysing data collected from local news websites as well as the company's annual reports aided our understanding of how e-Business activities have emerged in the company. Prior to 2005 the focus was on internal automation in the company, and thus very simple services were made available to the customers through the company's website. For instance, services such as viewing flight schedules, confirming reservations and tracing shipments through the Cargo system became available on the Internet. In 2005 the company signed a formal invitation to join the oneworld airlines alliance (Jordan Embassy, 2005) in which it committed to fulfill the alliance's technological requirements and work towards aligning its internal processes and procedures with these requirements. In 2007, in order to fulfill the oneworld requirement and officially enter the alliance, RJ went through a number of stages to improve and upgrade its IT, financial and administrative systems to be compatible and

linked with those operated by other companies within the alliance. Consequently, the following business-to-customer services were introduced:

- **The company website** was improved to include more information about flight schedules, travel procedures, and other information useful to customers (RJ news, 2006a).
- **Electronic Ticketing** was introduced to replace the traditional paper tickets.
- **Internet Booking Engine,** which provides customers with a convenient way to search, book and pay for tickets over the internet.
- **Self-Service Kiosk** which acts as a virtual operator for customers to self-check-in at the airport.
- **Royal Plus** which is a frequent flyers system to deal with frequent passengers and improve their service. It provides Frequent Flyers with information about their membership and the number of points they collect through traveling with RJ and other alliance members.

In addition to the previous business-to-customers services, and to meet the alliance's technological requirements, many systems were introduced to increase internal automation as well as business-to-business integration:

- **Electronic Purchasing System** was introduced to allow the company to communicate with its suppliers electronically and carry out all purchasing procedures over the internet. The company signed an agreement with Tejari, a B2B marketplace, in order to provide complete e-procurement services, which make it possible for RJ's various departments to send electronic purchase orders to the responsible section for electronic approval, and then send them to the supplier (RJ news, 2006b).
- **E-Management of Revenue** was introduced to help the company to optimise its profits. The system enables company to take future decision regarding travel classes, ticket pricing strategies, seat availability, ideal distribution of seats and prices in an optimum way (RJ's annual report, 2006).
- **Revenue Accounting System** was introduced to meet the alliance requirement for the electronic exchange of information between the members of oneworld as well as IATA members. It provides a more efficient way for managing and controlling

financial transactions. The system automates tickets sales and optimises the revenue accounting process (RJ news, 2006c).

Joining oneworld was considered as a turning point and the biggest achievement in RJ's history, as it was indicated doing so would have significant advantages for RJ (RJ annual report 2005). However, this massive technological transformation that the company undertook in a very short time[4] was not without security implications which manifested themselves in different social and technical aspects associated with the company's approaches to address e-Business security. From the study analysis it became apparent that security was not an integral part of the e-Business adoption process. At the strategic level it was not part of the organisation's plan to achieve its goals. At the operational level, some instances of the study showed that e-Business security was addressed in an ad-hoc manner based on purely technical controls. Aspects of the company's way of handling e-Business security and the factors affecting its particular approach will be explored as the discussion of the remaining emerged themes proceeds.

5.1.3 Organisational Structure and Security Function

Reviewing the organisational structure, roles and responsibilities through analysing the company's organisational chart and annual reports can provide useful information to explore many points related to the overall approach for addressing security in e-Business organisation, such as having security as part of the business strategy, management commitment, and support for information security in the organisation. RJ has a hierarchal-functional organisational structure with Chairman, President/Chief Executive Officer (CEO) and a board of directors. The CEO has a number of Vice Presidents (VPs) who are responsible for the various company sectors such as marketing, corporate finance, and technical sectors. Under each VP there are Heads of Department responsible for specific departments such as Information Technology (IT), Human Resources (HR) and finance. Departments are organised into sections/divisions which perform specific functions. Each section has its own manager who reports to the head of the department. Figure 5.1 shows part of the company's organisational chart (for simplicity, just a few sections and

[4] According to the Oneworld managing partner John McCulloch the implementation of the necessary changes was "quicker and more efficiently that we had ever expected": http://www.flightglobal.com/articles/2007/04/05/213076/majali-steering-royal-jordanian-into-oneworld.html

departments are shown). Reviewing the company's organisational structure and its annual reports, including strategy, mission, and vision, did not provide any evidence to claim that security was incorporated with the company business strategy or that it was perceived as a top management responsibility. Based on the previous data sources and interviews which were conducted with individuals from different organisational levels, the following observations were made:

1. **The Role of the Chief information officer (CIO)**: Prior to 2006, the company's organisational structure did not include the CIO role[5]. There was a head of the IT department who represented a contact point between higher management and the IT operational management. The CIO role appeared in the 2006 company organisational chart as a result of the number of organisational and technological transformations that the company undertook to fulfill the requirements for joining the oneworld alliance. The CIO coordinates interaction between top management and information technology management. CIO responsibilities include interpreting the top management strategy to the IT operational management, aligning IT projects with business objectives and other general management duties such as managing resources, budgets, and people in the IT department. No evidence from primary or secondary data has been found to support the idea that the CIO shares responsibility or is accountable for the information security in the organisation. The IT department, which was traditionally responsible for anything to do with the information and communication infrastructure, including information security, was divided into a number of sections, as show in Figure 5.2. From the study it became apparent that security related tasks were performed by the technical support section. These include configuring firewalls, access control for databases and operating systems, and reviewing the specifications of the new applications that the company intended to purchase. These tasks were performed by the technical support team in addition to many other technical tasks they performed in relation to the company's IT infrastructure. After 2006, a new division within the technical support section was established to be responsible for information security in the company. Also, the role of Chief Security Officer (CSO) was

[5]Based on reviewing the organisational charts in the company's 2002-2006 annual reports.

introduced as a position for the person who will lead the information security division.

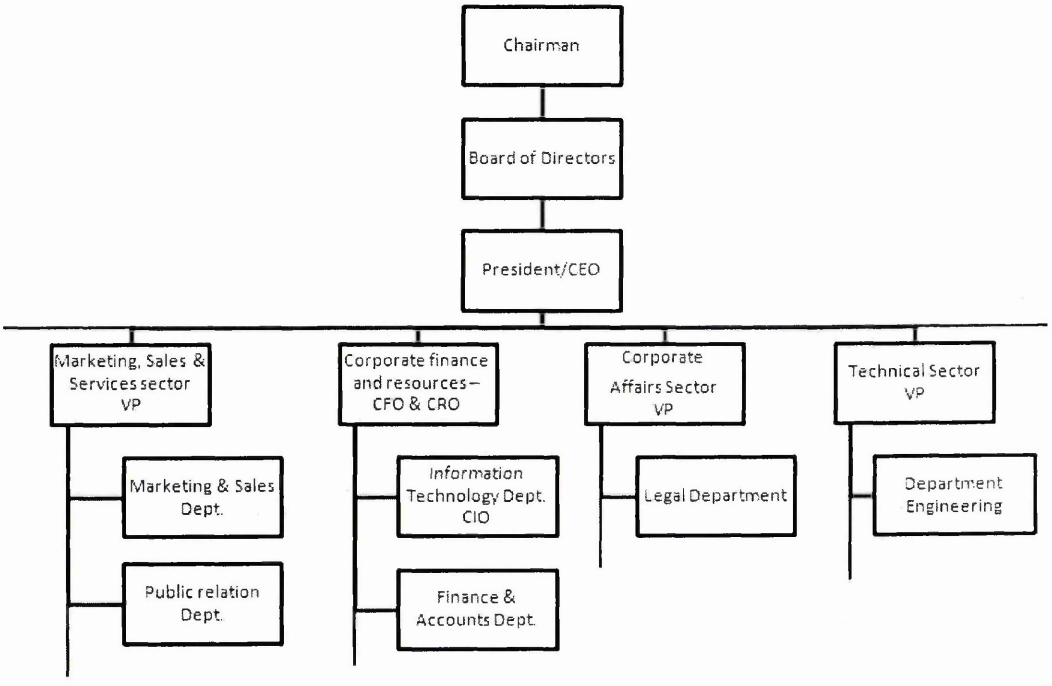

Figure 5.1: Part of the company organisational structure (adopted from the company organisational chart shown in 2006 annual report).

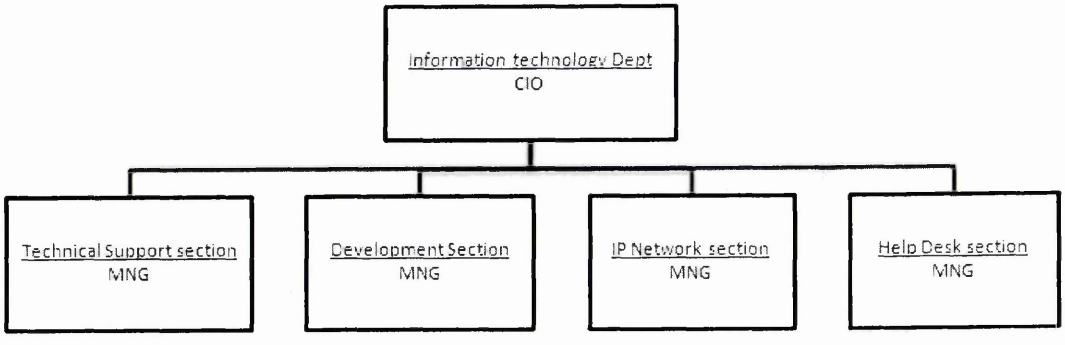

Figure 5.2: The IT department structure

It became clear that with the adoption of many e-Business applications combined with increased complexity of the IT infrastructure, outsourcing requirements, and emergence of new security threats, the technical support

section started to feel that they should have a dedicated team to take on the responsibility for security:

"In the legacy systems we were using a mainframe. That's why security wasn't a problem. Access was very restricted. The security threats started when we started to sell e-tickets. Because this means you need to give external access to the database. In addition to that the ticketing systems were hosted in a third party, therefore, we needed to agree with the third party on the security of such systems".

Introducing the security division at a later stage gives an example of reactive management which in fact did not help the security team and increased the complexity of its task in the company:

"As you know security cannot come at once, we have many systems and we cannot control it in few weeks. It takes about one month to review the security of a single system, so imagine if you are going to review all RJ's systems. We came at the time when all the systems in RJ were well established".

2. **The Role of Information Security Officers (CSO)**: The CSO is a newly established role to lead the information security division which has been established as part of the technical support section to be in charge of information security in RJ. After adopting e-Business applications and providing the customers with many electronic services, security issues started to surface more than at any time previously. One of the notable security issues, which caught the attention of everyone in the company, was the online fraud which appeared when the company started to accept online payment using credit cards:

"We were surprised when we saw the first fraud cases and we were wondering how this could happen. So we started to look for solutions and we have asked the airport stations to check the identity of people who paid through credit cards".

Such security issues combined with some compliance pressures from external stakeholders represented by the online payment provider, acquirer, and customer's banks, created some kind of awareness of the need to have a dedicated security team to help the company to improve its security. These stakeholders were pushing for implementing security standards such as the Payment Card Industry (PCI) standard to ensure secure transmission, processing, and storage of the financial information associated with online

transactions. According to the Information Security officer (CSO), these were the reasons for establishing the information security division:

"At the time we started to provide e-service they had to comply with standards such as PCI and RJ started to think how this can be achieved? Therefore, our section has been established to take the responsibility of supporting RJ in the security standards compliance. The connectivity between our systems which are distributed in different countries was an issue. All this made RJ think about security".

A number of tasks have been assigned to the CSO and his small team; these include: reviewing security standards to see how they can help the company; reviewing the security of the current system; and preparing a security policy draft, which was not in place at the time of this field study.

3. **The Role of the Information Security Committee**: During the field study there was talk about establishing an information security committee. During interviews with a number of management level participants from both IT and business sides, it was stated that the company was on the way to establishing this committee, which will include members from IT, legal and human resources departments. However, the responsibilities of the committee's members and how they will interact in relation to information security were not clear. From the study analysis it became apparent that many departments in the company were not supportive of previous security initiatives. For instance, although a draft of the information security policy was ready six months ago, it was stated that the technical support section was the only section which showed interest in getting this policy ready. This could justify the need for such a committee; however, it was stated that without giving this committee the power of decision making and top management support it was unlikely to be effective.

5.2 Operating Environment and Identification of Security Stakeholders

The adoption of E-Business has changed they way of doing business in the company, and many organisational and technological changes have been noticed in the course of the last five years. As discussed previously, many e-Business applications have been introduced covering all e-Business modes including B2C, B2B, and internal automation. At an organisational level, new functions and sections have been introduced, such as e-Business and e-Marketing sections, to cover the new business areas. Additional channels became

available for the customers to get company services, including e-mail, call centre and the company's website. Moreover, the company started to deal with a large number of external third parties including suppliers, technology providers, banks, and international bodies. All these changes made the company's operational environment more complex than at any time before. The number of interactions increased as well as the number of stakeholders involved in these interactions.

However, these changes had implications for security and increased the number of stakeholders who could affect or be affected by the security of e-Business. From the field study notes and interviews with participants from different departments, the researcher was able to construct Figure 5.3, which shows the company's e-Business environment and the different stakeholders and their interrelationships. Using a real scenario from the case study, it was possible to identify a wide range of internal and external stakeholders and their interrelationships. The scenario is presented below.

Stakeholder identification scenario: e-Commerce and the emergence of online fraud

In 2006 the company introduced e-Ticketing. It was stated that this would be more convenient for ***customers*** and it would speed up their travelling procedures. According to the company's 2006 annual report, introducing paperless ticketing was in line with the ***International Air Transport Association (IATA)*** regulations which banned the use of paper tickets in 2007. This was one step in the process of adopting e-Business. To fulfil the requirements of joining the ***oneworld alliance*** the company had to upgrade many of its systems to conform with the systems used by members of the alliance. In order to speed up the adoption process and meet the looming deadline for joining the alliance, many of these systems have been purchased and hosted with ***third parties services providers***. For instance, the Internet Booking Engine (IBE) and the company website were externally hosted. During the implementation of these new e-commerce applications, the company had only a short time in which to get an ***e-payment service provider*** to be integrated with the IBE. One of the participants stated that "*there wasn't time and they had to buy the systems as soon as possible...They got a payment gateway called PayPal and what was surprising is that PayPal has many problems*". One of these problems was the lack of a fraud screening mechanism, which later had security implications for the company's e-Business. As was the case in most of the new systems, the ***IT department*** was involved in the process of

selecting the e-payment provider. As a result the company's website was upgraded with all the new services and the responsibility of managing its contents was given to the ***e-Marketing section***, which was also responsible for communications with online customers. E-Marketing staff used to refer to the ***legal department*** to review anything they wanted to publish on the website, especially the privacy policy.

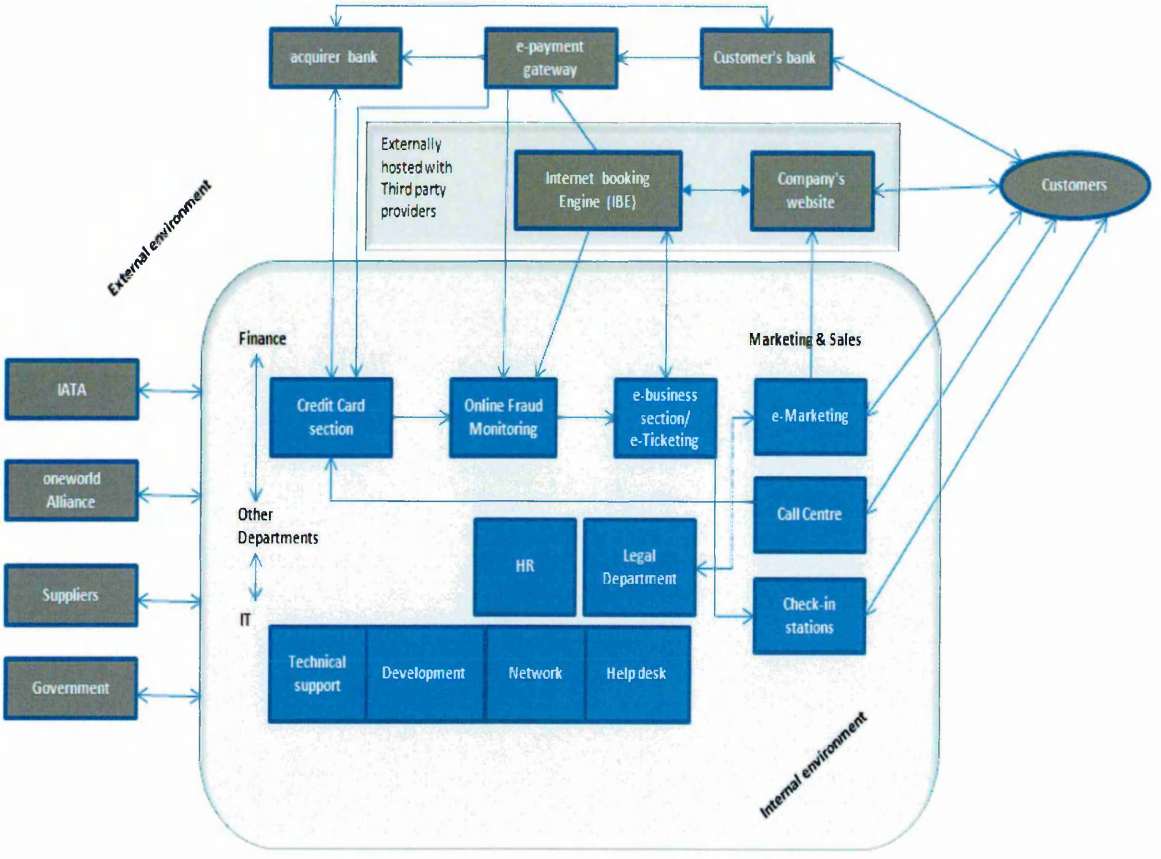

Figure 5.3: Operating Environment and Security Stakeholders (constructed by the researcher based on field notes and interviews with different stakeholders).

When ***customers*** started to use the IBE and pay over the internet using credit cards, the company started to notice an increase in the chargeback claims which were the result of online fraud. The chargeback claims were sent by the **banks** on behalf of the customers who denied purchasing online tickets using their credit cards. Because the company was unaware of this kind of threat, there was no protection mechanism in place and no information was collected to prove whether the customer who submitted the chargeback was a genuine customer or not. Hence, the company could not reject these chargeback

claims and its acquirer bank refunded those customers. The lack of knowledge about such a security threat was clear in many participants' interviews, for instance, the key participants from the financial department described it by saying:

> *"We were surprised when we saw the first fraud cases and we were wondering how this can happen. So we started to look for solutions and we have asked the airport stations to check the identity of people who paid through credit cards".*

Because the company was new in the field and it was the first time it experienced such a problem, it got back to the ***e-payment service providers*** and found that it could use a fraud screening tool, which in fact was very primitive and depended on daily retrieval of transaction information from the IBE and the payment gateway.

An ***employee*** (fraud monitoring agent) in the ***finance department*** was responsible for monitoring this information: that is, to check if there was any suspicious transaction which could be fraudulent. Once such a transaction was found, the fraud agent sent an email to another ***employee*** in the ***e-Ticketing section*** who then sent an e-mail to the ***check-in stations*** in the airport to suspend the ticket. To increase security, ***employees at the check-in stations*** were required to check the customers' credit cards and collect the cardholder information to make it available to the ***credit card section*** which could use this information to reject the chargeback claims. At the beginning of adoption, the number of transactions was very small and it was easy for the fraud monitoring agent to check these few transactions. When the number of online customers started to grow it became very difficult to check all the transactions and the chance of human error, as the process was partially manual, increased. A responsible employee commented on that by saying:

> *"As you see it is very slow and there is huge number of transactions. It is very difficult for me to look at all these transactions in this manual way. Previously, there were few transactions and it was possible to me to go through all of them".*

This also demonstrates how usability (or complexity) of the security tool can negatively affect the security of the system needing to be protected. Additionally, in many cases the credit card section failed to provide the bank with any evidence to reject the chargeback claims simply because the employee at the check-in counter did not collect the credit card information. Thus, staff negligence was another reason the effect of online fraud increased.

The company took some time to realise that it was unable to prevent the complex problem which was underestimated by both ***IT and Business managements*** who thought that the problem could be solved by a simple technical solution. When the ***management*** felt how much more serious the problem was, and the company encountered significant financial losses because of the online fraud, the ***IT department*** as well as the ***e-Business section*** were requested to look for an alternative solution. The implications of online fraud were clear in many participants' responses. One of the participants stated that, "*Till now the company is suffering from security problem. It is suffering from the credit card fraud. There are many chargeback cases. We lose money because of such chargeback and fraud cases*". During the field study, it became apparent that company is looking for a new e-payment provider who will be liable and responsible for monitoring online fraud. This was considered as new management style to deal with security. As one of the technical managers commented:

> *"In this way I think we can eliminate the risk by moving it from our side to the third party side. We were more reactive in fighting the fraud cases but now we are trying to be more proactive".*

However, it was noticed that this affected managers' perceived responsibility toward e-Business security. Dumping security responsibility on the provider's side appeared in many managers' interviews. For instance one of the business managers stated that the "*IT department have nothing to do with the credit cards fraud...as e-services is hosted externally*". This also was clear in another comment made by one of the IT managers:

> "*I told you I don't care about the security of my e-Business because it is ensured by somebody else. I have services providers who take the responsibility of ensuring security so that's it*".

Other stakeholders identified during the field study were ***internal auditors*** and ***government***. According to participants from the IT department, there was no password creation procedure or mechanism to force the staff to change their passwords until the ***internal auditors*** requested IT to force employees to change their passwords periodically. Additionally, it was clear from the study that ***government*** and ***national regulatory bodies*** are not meeting the expectations of the private sector in respect of e-Business. Many participants stated that the government is still far away and not fulfilling it responsibility to protect both business and customers:

"I think government is far away in respect to security. And this is the reason why there is a delay in regulation... It is vague no regulation or guideline to clarify that. I don't see any thing from the government side in relation to security. Nobody checks if the business capable from the security point of view to do business over the internet".

From the previous scenario, multiple stakeholders have been identified. These stakeholders have been classified into **Internal stakeholders** and **External stakeholders** (see Table 5.1). As this case study focus on exploring security perceptions in e-Business organisations, the identification of internal stakeholders was a very important step and a prerequisite for analysing these perceptions. The external stakeholders represent other units of analysis in this research which are covered in other chapters. However, considering all the stakeholders and searching for any evidence to understand their security roles and interactions is important in every unit of analysis to allow the researcher to construct a bigger picture of e-Business security.

Table 5.1: Internal and external security stakeholders.

Internal stakeholders	Examples
Top Management	CEO and board of directors
Information Technology (IT) Management	CIO, CSO, development and technical support managers and other IT managers
Business Units Management	Different units mangers: e-Business, HR, Credit Cards...etc.
IT staff	Admins, technicians, programmers, network engineers...etc.
Non-IT staff	Staff from sections such as marketing, finance, customer services and check-in counters.
Other internal stakeholders	Legal advisors who review the privacy policy and Internal Auditors who some time request increasing the security of the financial systems.
External stakeholders	
Customers	Online customers who use the company online services.
Services providers	Providers who provide services such as e-payment, hosting and e-Business applications.
International bodies	IATA and oneworld alliance.
Government	several governmental and regulatory departments that need to be involved and fulfil their responsibilities toward e-Business

To get more insight into the different security stakeholders and to fulfill the quest of this study to explore security in e-Business organisations, the internal stakeholders' perceptions have been explored and presented in the following section.

5.3 Analysis of the Internal Stakeholders' Security Perceptions

After identifying the company stakeholders, it was necessary to analyse the internal stakeholders' perceptions of e-Business security, as this study seeks to explore how e-Business security is perceived by these stakeholders, what affects these perceptions, and what the implications are for e-Business security. To explore security perceptions, many overarching topics covering e-Business and information security aspects were discussed with the study participants who were from different stakeholder groups. From the analysis of these interviews, a large number of themes emerged covering the different stakeholders' views regarding e-Business security in the study context. These have been compared, refined, grouped and classified into eleven themes and two general categories. See Figure 5.4.

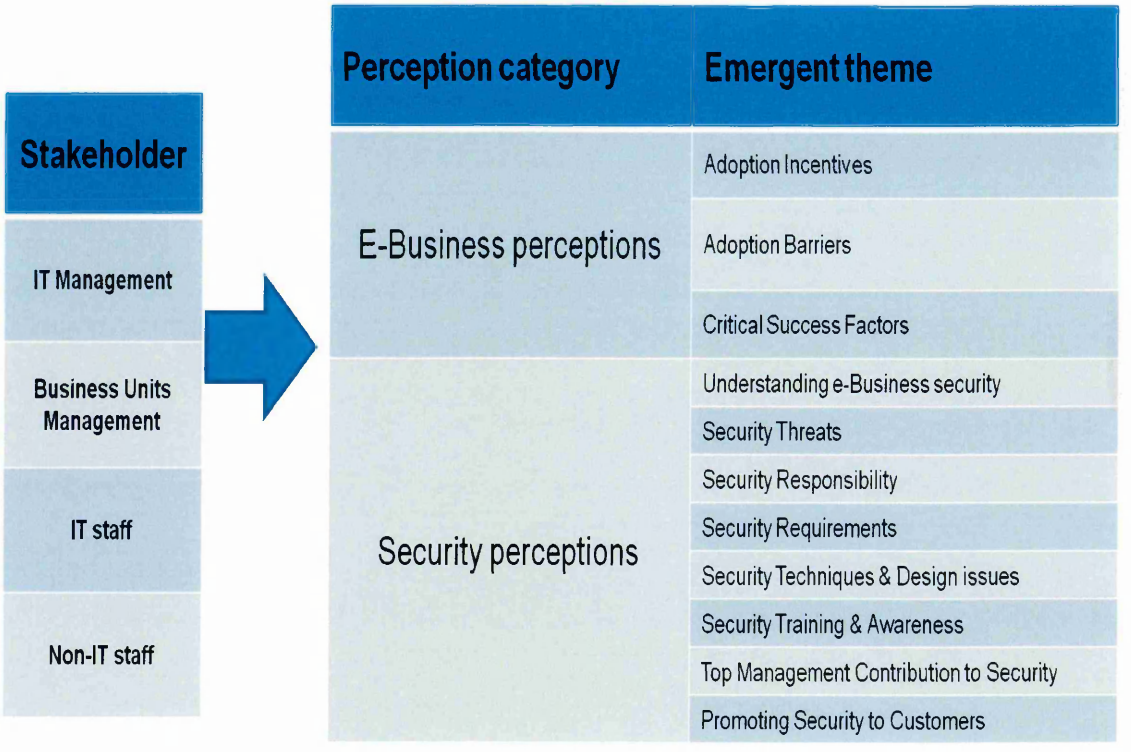

Figure 5.4: Themes which emerged from analysing the internal stakeholders' perceptions.

The discussion that now follows has been subdivided into four sections reflecting the four stakeholders: section 5.4 presents technology management's perceptions; section 5.5 presents business management's perceptions; section 5.6 presents IT staff's perceptions and section 5.7 presents non-IT staff's perceptions.

5.4 Views of Technology Management

To explore security perceptions and interests of this group of stakeholders, individuals holding management positions related to managing the company ICT infrastructure were interviewed. Details of their positions are shown in Table 1, Section 2.1. The researcher followed the case study protocol which was designed to cover the different dimensions of the problem area. Accordingly, technology managers were asked many questions to reveal how they perceive and deal with e-Business security. To ensure that participants were not influenced by the researcher's perspective or by the way of constructing the questions (which could lead them to provide a specific answer which might not reflect their real perceptions), the researcher started with questions not explicitly asking about security. For instance, participants were asked about what motivated them to adopt e-Business, what issues faced them during the adoption process, or the issues that they believe surround e-Business, and what they think are the critical factors necessary for successful e-Business. During the discussion of these topics, participants were probed to clarify some of the points which could lead to exploring some security perceptions. After that, the researcher started to ask more specific security questions which touched on the different aspects of e-Business security. As shown in Figure 5.4, many themes emerged depicting technology management perceptions about e-Business and security. These are presented below.

5.4.1 Adoption of e-Business: perceptions

Three themes emerged covering important e-Business aspects: adoption incentives, adoption barriers and critical success factors. These formed the category of perceptions of e-Business adoption.

Adoption incentives

From analyzing the technology management responses it became apparent that there were a number of driving forces that motivated the company to adopt e-Business in many of its business aspects as discussed previously. During the discussion many reasons were identified as adoption incentives. For instance *customer satisfaction* was mentioned by most of the participants in terms such as "making customer procedures as easy as possible", "providing the customer with good and convenient services", "instant communication with customers", and "providing them with all the possible technologies that satisfy them":

"Currently we try to improve our systems as well as getting some new systems in order to support the customers and provide them with convenient e-services. Now we have internet booking engine and self-service. We are willing to provide anything to our customers given that it will create customer satisfaction and reduce our overheads".

Competition and dynamic business environment is another reason which was identified by the respondents to encourage the company to adopt e-Business as a mechanism which would give the company power to keep pace with changing demands and high competition in the business environment. One of the key participants argued that *"Nowadays you don't have the choice of not having e-Business. We are in very dynamic environment and there is a high competition in this environment where you need a very fast reaction"*. *Improving business performance*, *increasing accuracy* by reducing human intervention and *generating revenues* were other adoption incentives stated by respondents. However, reviewing company annual reports and observing its e-Business transformation process revealed that the *most important adoption incentive was from an external stakeholder* represented by an international airlines alliance - oneworld. Joining the alliance was considered to be a turning point and the biggest achievement in the history of RJ, as it is indicated to have significant advantages such as image, competitiveness, and number of passengers. This also evident in the answers of some respondents who stated that joining the alliance motivated them to change business practices and introduce many online systems to fulfill oneworld's requirements. In one argument it was stated that *"in order to be able to communicate with these large companies you should have e-Business. So the integration is very important because we have many inter-transactions"*. Another participant clearly mentioned that by saying:

"One of the important requirements to be able to join the OneWorld was to change our way of doing business to meet the OneWorld standard. So we had to change four main systems in RJA and to connect these 4 systems to other airlines companies. Within 13 month we were able to accomplish all the transformation".

In 2005 the company signed a formal invitation to join oneworld and started the transformation process to fulfill the alliance's organisational and technological requirements as soon as possible in order to be able to meet the looming deadline, which was set to be the beginning of 2007.

Adoption barriers

From the technology managers' responses it was clear that the adoption process was not smooth; technical and social difficulties were experienced by the company. According to them the first issue was related to *interfacing with the company legacy systems*. As discussed previously, the company's computing power was based on the mainframe computer which hosted all the company's data and applications. At the beginning of the e-Business adoption process, which was very notable after signing the oneworld invitation, the company tried to integrate its legacy systems with the newly introduced ones. For several reasons identified by the participant this integration failed to work properly and delayed the company's adoption of e-Business:

"The most important obstacle we faced was the interfacing. There were legacy systems and the interfacing with them is not an easy task. This obstacle delayed us from utilizing e-Business".

The mainframe could not meet the high speed and instant transactions required by the alliance. Therefore, the company moved into the client-server architecture which provides an efficient way to communicate with the other airlines companies within the alliance. Other stated issues such as *lack of accuracy and absence of business process* in the legacy system made the interfacing a very complicated task. Therefore, the company found itself in a situation where it needed to replace many of its old systems which were *customised* to suit RJ's internal requirements without considering the requirements of other external stakeholders:

"One of the problems that all our previous systems were customised to suit the RJ internal rules and requirements without consider any external organisation such as IATA or oneworld. When we moved to online business we had to comply with their regulations and any system we buy should comply as well. This changed the way of doing business in many departments".

For technology management, introducing e-Business applications implied new business practices which were not necessarily the same as the old way of doing business in RJ. However, it is mentioned that many business unit managers and employees *resisted changing* their way of doing business and in some cases several customizations have been requested on some applications, not to improve business practices or meet standards but to meet the traditional way of doing business. Participants believed that *IT's lack of power to force changes* increased the effect of staff resistance to change. The process of introducing

a new system or business practices was not approved by the unit manager until the top management became involved and discussed the matter to get it approved. According to the respondents this process usually took time and delayed the adoption process:

"Employees resisted these changes and wanted the systems to be customised to meet their old way of doing their job. In IT department, we don't have the power to force any procedures or changes that why the process take time until the top management discuss the matter with the other department manger to get the new things approved".

Other external barriers emerged from their responses related to *customers' culture* which is not ready yet for e-Business. Cultural barriers such as awareness of e-Business and lack of trust prevented RJ from fully benefiting from some of it e-services. For instance, the lack of awareness and trust in the self-check-in kiosk prevented many customers from utilizing this service and forced RJ to assign someone to encourage customers and provide them with guidance to use the supposed self-service. *Security* was only mentioned by the Chief Security Officer (CSO) who stated that the information security section had been established to help RJ comply with security requirements and standards. This gives some indication that security is perceived as a barrier; however, it does not prove that it was properly addressed before or during the transformation process, as will be discussed later.

Critical success factors

After exploring the reasons which encouraged the company to move into the e-Business environment and the issues which hindered the adoption process, we now start to explore the perceived critical success factor for e-Business in RJ. Having security rarely mentioned as a barrier in the previous theme, and before asking the technology management explicitly about security of e-Business, it was difficult to judge whether or not security received enough attention from the beginning of the adoption process. Therefore, the question about critical success factors was another attempt to explore this point. Some respondents regarded *e-Business strategy* which clearly defines the company vision, goals and objectives regarding e-Business, as an important factor for successful e-Business, as it was stated that *"e-Business need clear management vision about what they really want from adopting e-Business"*. Also, *"skilled employees"* who are equipped with training and adaptable to any business change were considered as a critical success factor. Other factors such as *customer relationship management*, *ease of use*, *business process reengineering* and *strong*

infrastructure were mentioned by participants. *Security* appeared once in the respondents' answers. However, another single security aspect was regarded as a critical success factor. This appeared in the answers of some participants, who mentioned that *"having the information accurate and updated is very important for successful e-Business"*. Accuracy can be mapped to the integrity aspect of e-Business security.

5.4.2 Security perceptions

After discussing the previous topics with technology managers, it was necessary to explore in depth their understanding of e-Business security and its related issues, such as the meaning of security, security threats, and responsibility. Also it was necessary to explore how security is addressed in day-to-day business activities, therefore, questions continued to cover issues that are related to top management's involvement in e-Business security. Themes which emerged are presented below. The discussion of the perceptions follows in headings that reflect the themes which emerged, as labelled in Figure 5.4.

Understanding e-Business security

To exploring how technology management perceived security, participants were asked what e-Business security meant for them and how they dealt with it in their business environment. It was clear that there is a common appreciation for security, but what was interesting is the wide range of answers and how security means different things to different people in the same working environment. For instance, some participants perceived that security is only *related to the financial transactions* in which money is directly involved and there is a need to protect financial *information integrity* and prevent any attempt at fraud:

"*As e-Business it means conducting business over the internet and its security I think it is related to the financial transactions and using the credit cards*".

For others, e-Business security meant preventing company information from being disclosed to competitors or penetrators; it seemed only the *information confidentiality* aspect was understood by them. The need for *physical security* mechanisms such as cameras and door access controls seemed understood by most of the respondents; however, it was stated that physical access control was not in place in some sites until incidents which disrupted the business had been reported there:

"In one case one of the cleaning staff slept in the main tower and while he was sleeping he pulled a main cable and switched off all the airport and it took more than two hours to figure out the reason behind that. So physical security is important".

This gives the indication that security was overlooked in many business areas. Despite the fact the security issue in the computing environment is by no means new, it was stated the security was not problem and it only emerged when the company decided to go online:

"Previously we were using modems with speed of 1200 bps and all the systems were terminal emulation and everything was closed. There were no threats at that time... When our PC network started to grow and we got connected to the internet things became more complicated from the security point of view".

According to them, the previous systems were closed and less complex, hence security was not a big deal. Moreover, it was believed that these emergent security problems could be *solved technically* by implementation of required third party solutions. However, it was stated that *security is a complex, time consuming process* and *costly*. Although some respondents considered products come secure from the vendors who take care of their security, other believed that vendors do not pay that much attention to software security. Few participants were able to show comprehensive understanding of e-Business security, believing that security is *both technical and people issue* and *involves different parties* such as customers, suppliers and business who need to be considered when addressing security. For instance, it was stated that *"You have to make sure that your customers and suppliers are secure as much as you are secure, it is both interest"*, another participants argued that *"e-commerce security is about encryption, digital certificates, payment gateway...etc. this is the technical side. Inside the company it is related to the people"*.

Security threats

Security threats which come from outside the company boundary, such as *"network penetration, online fraud, viruses* and *natural disasters"* were the ones most cited by respondents. Some of these external threats had been experienced by the company in the past during the early days of deploying the internet in RJ. Some technology managers still remember when the *"Code Red"* worm hit the company network and how difficult it was for the IT department to isolate and solve the problem which took several days. It was stated that the lesson learned from this incident is that the company should have a strong

and updated anti-virus system. After this incident several changes were made to the network architecture to keep the network available even if some of its parts might get infected. Another external threat the company is still suffering from is the online fraud which emerged when the company started to sell over the internet. After the company tried to prevent fraud cases it realised how complex this is, and that their internal controls and experience were not sufficient to thwart online fraud. Therefore, it started to look for a new online payment gateway which would be completely responsible and liable for fraud cases. Inside threats seem to have been underestimated by the technology managers as the whole focus was only on the previously-mentioned threats. Although some of them believe that there is a need to "*build the employees security knowledge and they should understand its value*", respondents did not mention risk from internal staff as one of the main security threats that could affect the company.

Security responsibility & reference source

From the participant answers it became clear that security is perceived as an *IT responsibility* and this is widely accepted by most of the technology managers. This perception also seemed to be fostered by the technical orientation toward security:

"*I think IT department is responsible for that since all the security solutions and products come from the IT department.*"

This perception of responsibility for security shows the technical orientation of many IT managers who believed that security is merely a technical matter which only the IT department could take care of. Few considered responsibility for security as a shared responsibility in the charge of everyone in the company. For instance, one participant argued that "*everybody, from the cleaning staff to the CIO is responsible for security. The responsibilities may differ but everybody is responsible*". However, inconsistency started to appear when respondents were asked about the source of reference regarding what is allowed or not in relation to information processing in the company. Responses varied and included referring to the technical support section and human resources department. Yet some of them gave no clear answer. Others stated that "*each department has its own reference*". It became clear from the analysis that the absence of a security policy, which left security subject to personal judgment, affected perceived responsibility toward security:

"*Many people don't know what their responsibility is since there is no policy in the company defining that...So how do you expect me to punish or report any abuse or whatever related to security*".

Security requirements

Prior to joining the alliance and the adoption of e-Business, RJ depended on the in-house IT development team to develop its applications. Participants described some of the development stages such as design, implementation, and testing, and it was clear that different internal stakeholders, especially end users, were involved in this process to ensure the system would succeed. However, it seems functionality and design requirements were the main reason behind involving the other stakeholders. Security requirements were limited to specifying users' roles in the system in order to create an access control mechanisms:

"*Usually we consider the system requirement when we design any system. We look who is going to use it and what are the privileges s/he needs*".

Participants argued that in-house development was not an easy process, requiring resources, time, and effort in addition to the difficulty of meeting deadlines. It was stated that when the company began the adoption process and started fulfilling the technological requirements of the alliance, the in-house development was not capable of meeting the new demands which needed to be done in a very short time. Therefore, the company decided to use third party products and the development team started to act as facilitators for vendors who came to implement their solutions in RJ. In both the current and previous situations, the technical support section - in addition to many other duties - was in charge of the technical security requirements such as access control and authentication mechanisms. However, the company has recently established an information security section within the technical support section to be responsible for information security in RJ. However, the role of the security team, which has only two members, was not clear to many in IT as it was not involved in e-Business projects which were already in place when this security team came to the picture:

"*Actually we have CSO role which has been established recently but still we don't know exactly how he can help in our e-Business projects. Usually the product manager involves in the whole process in collaboration with the vendor*".

Security techniques and design issues

When we asked the development team about applying secure programming techniques and reviewing the code for security purpose, the answer was that "*the development team doesn't have an idea about that and there are not enough senior programmers to do the code review*". Regarding the company website, which is the first contact point for online customers, there were limited technical security features (e.g. SSL) which are not enough to secure e-Business or make customers feel secure while using the company website. From reviewing the website, there is no evidence of using trusted third party logos or security messages to inform the user about the level of site security. Also, it was found that there was no input validation for the information that the customer may enter in the website, which could cause security problems for both customer and company. When participants were asked about that, it was stated that the IT department is only responsible for the functionality of the website; design and contents are the responsibility of the marketing team who decide what to put on it and how it will look:

"We have the technical support section which provides us with all the technical details related to the security. We just provide the functionality and as appearance it is the responsibility of the commercial section".

Also, it was clear that there was no collaboration between the IT department and the commercial section to improve e-Business security. One of the technical managers stated, "*They [commercial section] decide what they will tell the customer. We don't have any say in the commercial things*".

Staff security training & awareness

Many participants emphasised the need for raising security awareness of the staff and building their security knowledge. Many incidents, related to passwords and e-mail security, were mentioned to demonstrate how employees' lack of awareness could cause security breaches. For instance, it was stated that "*employees shout their password over their desk partitions. Many employees don't know how much it is dangerous*". While there were few respondents who believed RJ staff are aware about security, during the study it became apparent that there was no security awareness training in place. However, it was claimed that security awareness initiatives were proposed by the IT department a long time ago, but

nobody from the business management and the human resources department gave them any attention or support because they were busy with other things and – from their point of view – did not want to waste the time. In term of specialised technical security training for the IT staff, nothing seemed to be offered except the providers' workshop and training which is tailored around particular products and may not focus deeply on security. However, IT managers argued that the situation has been changed for the better and they are going to implement a security awareness program in the near future.

Top management contribution to security

One of the topics discussed with the IT managers was how top management could contribute to e-Business security. In general the top management was perceived as supportive: however, in one instance it was stated that it might not be fully aware about the concept of e-Business security and it was the responsibility of technology management to introduce the concept and raise the security awareness of top management:

"*Let's talk about the situation in general. When it comes to the information we don't have a culture that respects information privacy. My role is to build awareness regarding this especially to the board of executives. So we as IT mangers try to introduce the concept to them*".

Some respondents argued that security is not part of the company strategy or the decision making process and this is because top management values functionality over security and it could be busy with other priorities:

"*Till now I couldn't refuse any product because it is not highly secured. They [Top management] always put the functionality in the front...Security is not part of the decision making*".

One of the points that arose from discussion was the need to empower the IT section, and this is one of the things that top management needs to address to enable IT to improve security. In many instances the IT managers stated that they were unable to introduce changes because of the lack of leadership and because decision-making powers have been given to business managers who are not aware of security. The effect of the top management was clear as many of the tensions between IT and business were not resolved until top management intervened. In addition to *IT empowerment*, respondents suggested other points to increase top management's contribution to security; these included *enforcing security rules and regulations*; getting the other departments involved in security

by *creating a security committee* which included a member from each department; *defining a clear role of the newly established security section*; and providing it with all the required resources.

5.5 Business Management Views

In addition to the previous group of stakeholders, a group of key participants holding management positions in the business area were interviewed in order to explore their perceptions of e-Business security. Similar topics were discussed with this group of stakeholders in order to compare them with the other internal stakeholders; however, the researcher tried to avoid deep technical probes which were not appropriate for business managers. Participants were from e-Business, Finance and Human Resource sections.

5.5.1 Adoption of e-Business: perceptions

In terms of e-Business adoption incentives, conformity was found between business management and the IT management, as similar reasons for adoption, such as customer satisfaction, reducing costs, and improving business performance, were mentioned. However, a significant difference can be seen in relation to the perceived issues and barriers during the adoption process. In contrast to the IT managers, the business managers argued that the transformation process was very smooth without any internal issues. The only perceived barriers were external, relating to online fraud and a customer culture that did not encourage the use of credit cards:

"*Another thing which is in fact a worldwide obstacle is the online fraud. Now we will change to another payment gateway which provides more option for fraud screening*".

An additional external barrier mentioned by participants was "*the culture that doesn't encourage people to use their credit cards to buy tickets over the internet*". Thus, customer's e-Business awareness was the only perceived critical success factor. From the e-Business point of view, only one aspect relating to e-Business security has emerged from the first part of the interviews. This aspect was related to online fraud which was perceived as external threat.

5.5.2 Security perceptions

Other security perceptions started to emerge when questions explicitly started to focus on e-Business security. These perceptions are presented below.

Understanding e-Business security

In the context of B2C, security seemed to be understood by business managers only in relation to online fraud, where there is a need for protection mechanisms to prevent this threat, which causes direct financial losses. For instance, when asked about e-Business security, it was stated that "*it means to reduce the fraud through use of security applications*". Internally, information confidentiality was the only perceived security aspect as it was stated that disclosing some financial information can harm the company. In general, the idea that security can simply be solved by deploying technical solutions was presumed by business management.

Security threats

Participants showed awareness of online fraud as a security threat for the company's e-Business. However, it was clear from their responses that this perception was obtained after this threat had been experienced many times. Consequently, the company decided to move to another e-payment provider who would provide extra security measures to reduce cases of fraud:

"As I told you we will move to another payment provider which has more fraud screening and authentication requirements. This is the only thing that we can do. We do some follow up for the suspicious cases. Daily we report about 20-30 suspicious transactions and we suspend many tickets. This is the maximum we can do".

Inconsistency was observed between business managers in relation to the perceived internal threats. While some of them believed that the internal business environment is secure and they need not worry about it, other participants argued that there is a threat from the employees who may exploit their privileges in a way that will harm the company. For instant it was argued that "*there is threat from the employee who knows the job. As much people understand the work there is a risk that somebody will exploit that for his own benefits, also there is a risk from the programmer who developed the applications that we use*". Compared to the IT

managers, they showed a very limited level of awareness about the diverse security threats that can affect the company's e-Business.

Security responsibility

Another inconsistency was observed in the perceptions of business management about responsibility for security. Some participants believed that Finance is responsible for e-Business security. Also, it was stated that *"the IT department has nothing to do with e-Business security because most of e-Business applications are hosted externally with a third party providers"*. In spite of that, in many instances it was stated that security applications have been requested through the IT department, as it appears in the following quotation taken from one the business managers who was taking about protecting e-Business:

"This is what we told the IT about, and they brought the tool to reduce that".

Other participants argued that the IT department is responsible for the technical details of security while both the legal and the human resources departments are responsible for security rules and regulations. None of the participants showed that security is perceived as shared responsibility.

5.6 IT Staff Views

Technical people including systems administrators, programmers, systems analysts, network technicians and engineers, represent another group of security stakeholders, as they are in the heart of the company e-Business infrastructure. Therefore exploring their perceptions was necessary to get more insight into the problem situation.

5.6.1 Adoption of e-Business: perceptions

Conformity was noticed between IT staff perceptions and the previous participants' perceptions regarding the driving forces that motivated the company to adopt e-Business. However, additional evidence was identified which supports the previous speculation that the primary driving force for e-Business in the company was from an external stakeholder, oneworld alliance, which put the technological transformation into an electronic environment as a prerequisite for joining and getting the benefit of the alliance:

"In 2005 OneWorld came to the picture. It required a very high speed and instant transactions. At the same time our mainframe could not meet these requirements. So the vision of the management

was to move toward more advance technology which has been deployed by many international airline companies".

Regarding barriers to adoption, IT staff only emphasised the issue of employees' culture and resistance to change which slowed down the adoption process. Participants stated that this issue is clear among the senior employees who were not exposed to the new technology.

5.6.2 Security perceptions

Similar themes emerged from discussing specific security topics with IT staff. These themes are presented below.

Understanding security

The impact of security on business was generally recognised by most respondents, who stated that insecurity has a number of negative implications such as "*financial losses*", "*customer turnover*" and "*business disruption*". When respondents were asked about e-Business security, there were no common answers and few respondents were able to provide clear definitions. Awareness of technical security mechanisms such as encryption, access control, and physical security was clear; for intake, it is stated that e-Business security means "*full system security including public key encryption, access control*". In contrast, some respondents were able to highlight the role of human factors in e-Business security. For instance, it was stated that security gaps could not be prevented completely since there is always a human (programmer, developer or user) involved in the process. These respondents argued that the effect of the human factors can be reduced if employees have good ethics:

"*We as programmers know the weaknesses in our systems and how it can be utilised to gain some personal benefits. Some programmers may give such information to somebody out side the company who can exploit these information get some service that he is not entitle to... I think you should be loyal to your work so it is an ethical matter*".

Security threats

In contrast with the previous respondents, IT staff showed an awareness of both internal and external security threats which could impact on e-Business. Some external threats such

as fraudulent transactions and network penetration attempts were mentioned. However, many participants argued that company employees are the main security threat:

"*If there are employees who hate the company for some reason, he may behave in a way that will hurt the company, for example by letting some private information to leak outside the company*".

Furthermore, participants mentioned the threat that employees, such as programmers and systems administrators, could intentionally abuse their privilege to gain some benefit:

"*The important threat to the company is internal and related to our own employees. We as programmers know the weaknesses of our systems and how they can be utilised to gain some personal benefits. Some programmers could give such information to somebody outside the company who can exploit this information to get some service that s/he is not entitled to*".

Also it was stated that internal users' negligence and lack of security culture are a source for many security breaches.

Security responsibility

Whilst some of the IT staff interviewed perceived responsibility toward security as an IT responsibility, other IT staff believed that security is everyone's responsibility. Some respondents argued that IT is responsible for technical security and unit mangers are responsible for enforcing the rules and regulations relating to security. Other participants argued that everyone who has access to company information should be responsible for security:

"*Everyone is responsible for his/her own data. So whoever has access to some piece of data should take care of it and ensure its security...Everyone shares this responsibility not only one section in the company. IT shares a big part of this responsibility since they build all the systems and know all the weaknesses in these systems. Also the end users share this responsibility*".

Compared to the previous groups of respondents, IT staff gave a more comprehensive view of responsibility for security.

Security requirements

It became clear that usually a number of stakeholders participate in e-Business projects undertaken by the company. According to the participants, these stakeholders include: project manger, developers, systems analyst, technical support, super user (the head of

department where the system is going to be used) and the vendor. The end user usually participates at a later stage for some testing and customization. The main task in which all these stakeholders participate is the elicitation of functional requirements. Regarding security, it was stated that it is only discussed between the vendor and the technical support to decide the technical details of security. In other instances, it was stated that security is included in the vendor products and the vendor has security standards to follow:

"*Usually we get the solutions for our e-Business projects from the vendors and security is included, however, we might tune them to meet our needs. We don't have the requirements in advance...*".

In addition to the previous findings, this clearly indicates that security was treated as add-on feature or module that can be added to the system to provide security. Also, it provides additional evidence for the lack of a security requirements process that covers all the needs of the different stakeholders.

Top management contribution

The analysis revealed that the IT staff believed top management should give security more attention and it should be considered as the first priority. Participants suggested many ways for top management to contribute to e-Business security in the company. For example, one of the participants suggested top management should support and enforce the decisions related to security. Another participant suggested that top management should provide financial support for security initiatives in the company. An additional suggestion was increasing the security team by hiring expert experienced security staff.

5.7 Non-IT staff views

To uncover all the perspectives inside the company, other groups of employees were interviewed. These included employees from the e-marketing, e-Business, finance and credit card sections. These participants are referred to as non-IT staff to distinguish them from the IT staff previously interviewed. We should mention that security related topics were not discussed in detail with all participants, especially this group, as they do not have a technical background and have not received security related training.

5.7.1 Awareness of security and security good practices

Limited security aspects were understood by the non-IT staff. Most of the respondents talked about the need to prevent the company's private information being disclosed. Some of them focused on protecting customers' information and other focused on the fraud cases that the company is currently suffering from.

"*It means that the company will not reveal customer information to any third party company. The company should protect the customer personal information*".

This gave the impression that the confidentiality aspect of e-Business security was the only aspect understood by the participants. As an attempt to explore their awareness of some good security practices in their workplace, we asked them how they usually chose a password and if they had any particular procedure which they followed to choose a good password. Few participants stated that in some applications the system gives the rules for creating a password. However, the majority stated that they chose whatever they want and usually they selected something very personal as they believed it would be more secure or easy to remember:

"*I choose my own password in a way that no one can know my password. [**How?**] I choose something very personal so no one can know it*".

Participants stated that they never received any training or induction course about anything related to good security practices. This fact could explain their low level of security awareness.

5.7.2 Commitment toward security

The only provision which we found in place to get the company's employees committed to security was in the job contract. Participants stated that they were required to sign a "*non-disclosure agreement*" which was part of their job contract. When they were asked to give more details of this agreement, they described it as "*terms and conditions*" that warn them about revealing private company information. Following the discussion of the previous point, this might explain why confidentiality was the only security aspect which was understood by and had the attention of the company's employees.

5.7.3 Security responsibility

Similarly, inconsistency was found between the general staff's perceptions of responsibility toward security. Some of them argued that the IT department is responsibly for security and should protect the company network from security breaches. Other participants stated that both the finance and the IT departments are responsibly for security. In one instance, it was stated that everyone in the company is responsible for security.

5.7.4 Promoting security to the customer

Most of the current and the previous participants raised the issue of customers' online distrust. When previous participants, especially those from the IT group, were asked if they promoted security to online customers to increase their trust, many of them argued that they did not have a direct communication with the customers and it was the responsibility of the commercial and marketing sections. Because some of the non-IT staff interviewed were from the commercial and e-marketing sections, it was interesting for us to ask how they communicate with customers and whether or not they give them any information about security. Respondents expressed how much communication is important in attracting customers and creating trust, and this was the reason for creating the e-marketing section, which takes responsibility for managing website contents and provides another channel to stay in touch with customers.

"*As much we try to be near to the customers through the reply to their feedbacks and communicating with them as much this increase their trust. If the customers' suggestions are reflected on our website they will trust us*".

They mentioned many ways that they usually use to communicate with the customer such as e-mails, feedback forms and the attractive ads that they put on the website. However, when we asked them if they promoted the security of their e-Business to customers through these forms of communication, for example by placing logos of some trusted third parties, some participants replied that they "*never think about it*" and other participants argued that "*it is not necessary to tell the customers about how much the system is secure. Any company by default should protect its e-Business*".

5.8 How e-Business security is addressed within e-Business organisation

During the field study it was clear that the importance of e-Business security was recognised by many of the internal stakeholders. However, for a number of reasons which will be discussed in the next section, this recognition was not reflected in the company's approach to addressing security. In general, security was treated as a merely technical problem and there was a wide belief that security issues could be solved by deploying various technological controls such as firewalls, anti-viruses, and encryption mechanisms. Such an approach has been described by von Solms (2000) and it has been demonstrated that this purely technical approach is insufficient as it fails to address many non-technical aspects which contribute to the security problems that many organisations are facing nowadays (Dhillon & Backhouse, 2000; Schneier, B., 2000). Moreover the analysis showed that this technical approach was implemented in an "ad-hoc manner without following defined processes or policies" (IT Governance Institute, 2006). From the field study it has become clear that there was no risk assessment process to identify security threats that might be associated with e-Business projects; awareness of such threats depended on individual stakeholders and was not communicated to other stakeholders at the different organisational levels; there was a lack of business processes and a dependence on third party products; and there was an assumption that technology providers provide an adequate level of security in these products. These together led the company to end up with a mind set of isolated silos, not able to see the whole picture, which increases the chance that many security threats will be overlooked.

Many instances from the case study showed that security was initially overlooked in many e-Business initiatives undertaken by the company. For instance, there was no fraud screening mechanism when the company started to accept online payments; this was added later after the company suffered from financial losses which were the result of fraudulent transactions. Authentication mechanism is another example showing that security was overlooked. In some applications there was no password creation procedure integrated with the authentication mechanism to force users to create strong passwords or change them periodically, as recommended by many security best practices and standards (e.g. ISO 27001). Such a procedure was added later when the internal auditors raised this issue with the IT department.

The two previous examples and other examples explored during the field study reveal that the company followed a reactive approach to deal with security. It is notable that security was an afterthought in different areas, including organisational structure, software acquisition, and physical security. At the organisational level the security function and the role of Chief Security Officer (CSO) was added at a time when all e-Business applications were in place. The relationship of the CSO with other organisational functions was not clear, and responsibility toward e-Business security was not defined. This was evident in the different stakeholders' perceptions regarding responsibility for e-Business security. In criticising such a situation, Posthumus and von Solms (2006) argued that information security should be part of the corporate governance and responsibility should be clearly defined at all the organisational levels to ensure effective information security function. Regarding software acquisition process, it became apparent from the study that functionality and ease of use were given more attention than security, which was added only after some security threat was experienced by the company or a specific stakeholder raised a security-related requirement. Treating security as an add-on component added at a later stage had many implications. For instance, adding the password procedure required customising all the interfaces for the applications required in this procedure. Similarly, an e-payment gateway was integrated with the company's website and customers started to use it without any fraud protection mechanism. When fraudulent transactions became a serious problem, the company decided to use a fraud screening tool. This solution was very primitive and was limited to a monitoring function which allowed the company to collect information about any suspicious transaction to be used in case of any chargeback claim, or to suspend the ticket associated with the transaction. The solution suffered from many issues, including design, usability, and integration issues, that contributed to increase the chance of human error (Kraemer & Carayon, 2006) that might lead to security breaches. Conflicting requirements were also notable; during discussion with the technical staff, it was stated that the level of security in the fraud monitoring tool was kept at a medium level to ensure availability. However, this increased the number of suspicious transactions which needed to be filtered. The issue of treating security as add-on component has been brought up by Baskerville (1992) who described the issue of development duality in which security is not integrated with the software development process which could lead to conflict and tension between a system and its security.

Having discussed the company's approach to dealing with e-Business security and its implications, the next section discusses the set of factors which influenced the company's security approach. In other words, answering the questions of why in this case study security was overlooked, why it came as an afterthought, and why it was perceived from a purely technical dimension. By giving detailed explanations of these "*whys*", the study provides an exceptional and comprehensive framework for understanding e-Business security in the context of an e-Business organisation in Jordan. From the study a number of conceptual elements have been identified: these elements were classified into security related concepts. In the next section, these will be used to develop an explanatory model that will be used to form a discussion to explain the relationships between them.

5.9 Factors affecting e-Business organisation security approach

By applying the inductive coding process on the raw data, text segments which represent recurring ideas related to this study's research concerns were identified. Initially, each group of recurring ideas with a common topic which can be used as an explanatory account was organised into a single concept or theme. For instance, all the text segments highlighting the issue and effect of top management's support of security were grouped into one theme labelled as "Lack of Top Management Support". In total, 37 conceptual elements or themes related to the study concerns have emerged from the analysis. These are shown in Table 5.2. These were divided into 4 security implications, which helped in describing the particular approach that the company followed in addressing e-Business security, and 33 explanatory concepts, which represented factors affecting the organisation's security approach.

Table 5.2: Emergent conceptual elements related to e-Business security.

	Explanatory Concept	*Location*
1	Lack of Top Management Awareness	CSO,CIO,PRM
2	Lack of Top Management Support	CIO,CSO,TSM,ITD,DSC,NTE
3	Lack of Effective Internal Communication	CIO,TSM,ITD,DCS,SIT,EBD,EBR, PRM
4	Lack of Effective External Communication	CIO,TSM,ITD,HDD,DCS,EBD,EMD,EME
5	Lack of Security Policy	CIO,TSM, HDD,NTE,NTT,TTS
6	Lack of Knowledge	TSM,ITD,HDD,PRM,WPRM,OPRM,CMM
7	Lack of Security Requirement Process	ITS,TSM,PRM,RS,WPRM, CSO,ITD
8	Lack of Internal Stakeholders Support & Commitment	TSM,ITD,DCS
9	Lack of Leading & Decision Power in the IT	TSM,ITD,DCS
10	Lack of IT Staff	ITD,RS
11	Internal Stakeholders' Conflict	TSM,ITD,DCS,EBD
12	Technical Orientation of Internal Stakeholders	CSO,NETM,HDD,DCS,CMM
13	Different Security Risk Perceptions	CIO,TSM, CSO, HDD, EBD, CCM, NTT
14	Perceived Security Responsibility	CIO,CSO,ITD,DCS,PRM,NTT
15	Perceived Complexity of Security	CIO,CSO,TSM
16	Perceived Cost of Security	CIO,NETM,ITS
17	Not perceiving Security as Competitive Advantage	CIO,TSM,EBD,EBE,EME,EMD
18	Appreciating Functionality & Ease of Use	ITS,TSM, CSO, PRM, NETM, FM
19	Lack of Staff Security Awareness Training	CSO,TSM,ITD,NTE,NTT,ITS
20	Staff Culture and Resistance to Change	ITD,DCS,RS,EBR
21	Staff Negligence & Human Errors	ITD,NTT,EBA,FM
22	Staff Malicious Behaviour	ITD,NTE,ITS,WPRG
23	Lack of Security Ethics	WPRG,NTE
24	Complexity of emergent technology	NETM,HDD,NTT,ITS,FM
25	Complexity of security and its tools	CSO,FM, FNA,EBA
26	Accessibility versus Protection	CSO, PRM, FM
27	Security of third party products	CSO, TSM, ITM,CCM
28	External Stakeholders Requirements	CIO,CSO,ITD,DSC
29	Looming Deadlines	CSO,ITD,EBA
30	Outsourcing to Providers	TSM,PRM,EBD,EME
31	Absence of Effective Government Role	CIO,CSO,TSM,ITD,HDD,DSC
32	Legal Uncertainty	LA, HDM
33	Lack of Security Legal Setup	LA, CIO, CSO
Security Implication		
34	Security was overlooked	NETM,CSO,CIO
35	Security was an Afterthought	CSO,TSM,ITD,NETM,HDD,PRM,OPRG,CCM,EBA
36	Ad-hoc Approach to Address Security	CSO,TSM,OPRG,EMA
37	Customer Distrust	CIO,CSO,TSM,EBD,CMM,EME,EMD

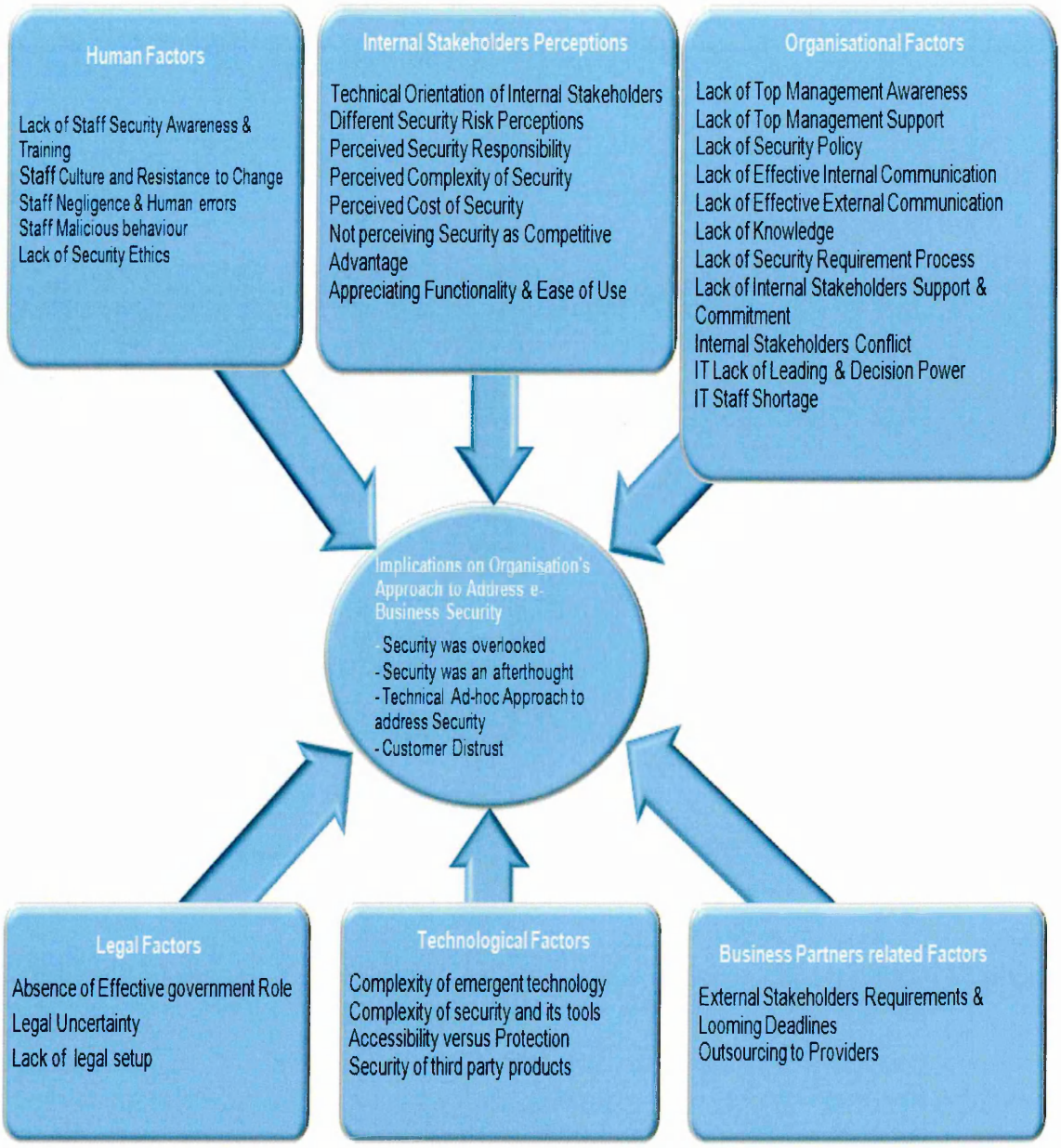

Figure 5.5: Explanatory framework of factors affecting e-Business organisation's approach to security.

To develop the theory explaining the problem situation further, security related explanatory concepts from Table 5.2 were grouped into more abstract concepts or categories consistent with the study framework of inquiry discussed in Chapter 2. This framework argues that different dimensions affect the e-Business security environment. It defines these dimensions in an abstract way and, by using the case study explanatory concepts and emerged categories, it can be grounded with concrete explanations and refined into a

coherent and explanatory framework, as shown in Figure 5.5. For example, all the emergent concepts relating to legal aspects of e-Business security have been categorised under one theoretical construct called "Legal Factors", which in turn can be mapped into the legal dimension in the study framework of inquiry. It is worth noting that exact mapping between the emerged explanatory framework shown in Figure 5.5 and the study's framework is not expected, as the latter is intended to provide a broad organising framework for conducting such a qualitative study.

As shown in Figure 5.5, the way e-Business security was addressed was influenced by multidimensional and interrelated factors; these include internal factors, which have been placed into three categories in the framework: *Human factors*; *Internal Stakeholders' Perceptions*; and *Organisational Factors*; as well as external factors, which have been categorised into: *Legal factors*; *Technological factors*; and *Business partner related factors*; these are discussed below.

5.9.1 Organisational Factors

Several organisational related issues have emerged from this study, including management, strategic, communication, and knowledge issues. These issues have been categorised into eleven organisational factors which have been found to affect the overall company approach to security discussed earlier. These included:

1. *Lack of Top Management Support*: Top management contribution to e-Business security was one the themes explored in this case study. The general effect of top management involvement was notable in different business areas. Many participants stated that technological changes could not be implemented without top management intervention and support. However, the study revealed that top management support and direct involvement in e-Business security was very limited. This was evident in many participants' arguments which suggested that top management should give security more attention and support. Actions such as incorporating security in business strategy, enforcing security rules and regulations, increasing the security team, and empowering IT have been suggested to increase the contribution of top management to improving security.
2. *Lack of Top Management Awareness*: Participants stated that functionality and performance were more recognised by top management whilst they were not fully

aware of the importance of security. Furthermore, they stated that it should be the role of the IT management to build top management security awareness.

3. *Lack of Effective Internal Communication*: Notably, security was not communicated between the stakeholders at different organisational levels. No formal reporting for security incidents existed. Only suspicious transactions and fraud cases were communicated between specific operational staff. Additionally, financial losses associated with fraud cases were reported to the top management. Lack of a common language of security was observed between groups of internal stakeholders. Furthermore, the role of the information security team was not understood by many participants.
4. *Lack of Effective External Communication:* Another security communication issue has been observed between the internal stakeholders and the external stakeholders (particularly, the company customers). From the study it became apparent that limited information about security was communicated to customers. Participants who have direct contact with customers seemed unaware of the importance of customers' security perceptions and how this could impact on their trust perceptions on the company's e-Business.
5. *Lack of Knowledge*: Lack of both e-Business and security related knowledge was another issue discussed by the participants. It was stated that when the company started to adopt B2B and B2C these were new business fields and knowledge about them was very limited even in the IT people. Similarly, the company was not fully aware of security requirements and the various threats associated with adopting e-Business, which led to a situation in which many security aspects were overlooked. For instance, participants stated that they did not have any previous knowledge about online fraud, and when the company experienced this threat for the first time, everybody was asking how this could happen. When asked about specific security topics such as applying secure programming techniques, IT members showed a limited awareness of such security topics, which also demonstrated a lack of knowledge about security.
6. *Lack of Security Policy*: An information security policy was not implemented in the company. The effect of the lack of a security policy was clear in the answers of the participants who were not able to specify a security reference source which was

documented and communicated to everybody in the company. At the time of conducting this field study, the IT department had started writing a draft information security policy, which provides additional proof that security was an afterthought.

7. *Lack of Security Requirement Process*: Regarding security requirements, there was no clear security requirement specification process in the projects the company undertook. Functionality and design requirements were more recognised in these projects. Limited technical security specifications have been handled by the technical support section. These were limited to specifying users' roles in the systems to create access control mechanisms.
8. *IT Staff Shortage*: IT staff shortage was another issue which affected the company's e-Business security. The information security team was very small compared with the tasks that they were expected to do. Increasing the information security team was one of participants' suggestions to improve security. When asked about reviewing software codes as a way to ensure security, participants argued that the IT department did not have enough senior programmers to perform such a task.
9. Other organisational factors identified were related to the relationship between internal stakeholders. As they were interrelated with each other, they will be discussed together:
    a) *Lack of Leadership & Decision-making Power in IT.*
    b) *Internal Stakeholders' Conflict.*
    c) *Lack of Internal Stakeholder Support & Commitment.*

Some tension and conflict were observed between some groups of internal stakeholders. Participants from the IT department argued that decisions were in the hands of business people who did not understand security and its importance. Also, they discussed how the lack of IT power made it difficult to introduce and enforce changes in the business environment. They believed that this affected security, as any security-related action needed to go through a number of convincing stages. On the other hand, business management believed that IT people have nothing to do with security of e-Business, as many of its applications are hosted externally. Business unit managers perceived IT people as enablers who should fulfil whatever the business requests from them, and many instances showed that the business people were not supportive of security initiatives and

did not like suggestions from the IT department. In summary, there is no decision-making authority in the hands of IT to enforce security in the business environment.

5.9.2 Internal Stakeholders' Perceptions

The study analysis showed that the stakeholders' security perceptions were important in shaping the company's particular approach to addressing e-Business security. Seven factors which affect security and are related to internal stakeholders' perceptions have been identified:

1. *Technical Orientation of Internal Stakeholders*: The technical orientation toward security was clear in many respondents' answers. Few participants showed understanding of the non-technical aspects of security. The majority believed that e-Business security can be solved by applying technical controls which they can get from third party providers. Accordingly, it was assumed that the IT department was taking care of security as it was considered extremely technical and only experts could get involved in it.
2. *Different Security Risk Perceptions*: Asking participants about different overarching security topics, such as what e-Business security means for them and what kinds of threats that the company could face, revealed that stakeholders who were working at the same place might have different perceptions of security risk. For some participants, security was only understood in the context of the financial transactions; however, for others, it meant protecting the company's information from being disclosed. Some participants overestimated the risk of some security threats, such as product security and employees' uncontrolled security behaviour. In contrast, others seemed unaware of that at all.
3. *Perceived Security Responsibility*: Responsibility toward e-Business security was not perceived as a shared responsibility. Moreover, inconsistency was observed between internal stakeholders' perceptions of responsibility for security. Some participants viewed it as a specific responsibility for a particular group of stakeholders, section, unit or department. Others felt less responsible for security as they considered it someone else's problem.
4. *Perceived Cost of Security*: Perceived cost of adding security was another factor which led to security being overlooked. Cost of security seemed one of the expenses

the company tried to avoid as no separate budget was assigned to security. Spending on securing business areas which generate less revenue seemed unjustified by number of participants. On the other hand, the cost of security breaches was underestimated, which could explain overlooking the risk of online fraud. One participant argued that if the cost of adding security is higher than the return from the place which needs to be secured, there is no need for strong security at that place.

5. *Perceived Complexity of Security*: Security has been perceived as a complex and time-consuming task. This perception discouraged some participants from trying to learn more about security. For instance, when asked about security, many participants stated that the topic is very professional and only experts can talk about it. Perceived complexity also appeared in the arguments of participants involved in security, as it was stated that reviewing a single system is not an easy task and could take a month. Having all the systems in place prior to establishing the security team made them feel that their task would be difficult. Also, it was stated that the process of monitoring online fraud was cumbersome and it was felt that the company was incapable of addressing such a complex issue.
6. *Appreciating Functionality & Ease of Use*: Other aspects, namely functionality and ease of use, were recognised and appreciated by the internal stakeholders more than security. Discussing several e-Business aspects with participants revealed that security had a low priority prior to and during the adoption process. During that discussion, terms such as "improving business performance" and "providing customers with easy, understandable and convenient services" were more cited as reasons. On the other hand, security was rarely mentioned, whether as a barrier or a critical success factor. Some participants argued that security is the last thing that management would think about as their decisions are solely based on functionality.
7. *Not perceiving Security as Competitive Advantage*: Security was not perceived as something that could attract online customers or build their trust in the company e-Business. This perception was held by many participants who had direct communication with customers. They argued that customers did not need to know about security as the company by default should ensure security. Consequently, no information about security was communicated to the company's online customers.

5.9.3 Individual/Human Factors

Employees are individuals working at different organisational levels and interacting with e-Business applications on a daily basis. Many human characteristics make their behaviour unpredictable from a security point of view. In the context of this study five human factors contributing to e-Business security problems have been identified:

1. *Lack of Staff Security Awareness & Training*: There was a notable absence of good security practices that general company staff can follow in their work environment. When non-IT participants were asked, they showed limited awareness of security practices which could help them to ensure security. Their understanding was mainly focused around information disclosure. For instance, many of them stated that they usually chose something personal for their passwords as they believed this would be more secure. The study revealed that general staff never received any security awareness training and most of their security related actions were based on personal judgement, which increased the chance of compromising security. The lack of security awareness and the need for building staff security knowledge were acknowledged by many participants who believed that this would help dramatically in improving security.
2. *Staff Negligence*: A number of security breaches mentioned by participants were due to staff negligence, without the intention to harm the company or to achieve personal benefits. Although they were usually requested to change their initial password, some employees were found using the initial passwords created by the IT department. Another case illustrating the effect of staff negligence was related to online fraud monitoring which, as participants stated, depended on collecting information from customers at the airport. However, there were many cases in which this information was not collected because of the lack of staff attention, and as a result the company did not have any proof to reject chargeback claims which were based on fraudulent transactions.
3. *Staff Malicious behaviour*: Other security breaches were due to intentional abuse of privileges given to the employee. In one instance, a programmer added a piece of code in the company applications, which made the application stop from time to time. Whatever his intention was, this represented a security breach which was a

result of malicious behaviour. The risk of malicious staff behaviour was acknowledged by participants who argued that there is a risk from employees who know the system or who are not satisfied with their jobs.

4. *Lack of Security Ethics*: Many organisations have some sort of ethical code to encourage acceptable employee behaviour while using computers in a business environment. Unfortunately, there was no such ethical code in our case study. When participants were asked how malicious behaviour by employees could be prevented, they argued that this is an ethical matter. They believed having some sort of ethic could help in preventing such issues, especially in the absence of rules and regulations to control security.
5. *Staff Culture and Resistance to Change*: Participants believed staff culture did not encourage security. It became apparent that their culture did not respect privacy of information, as it was stated that some employees shouted their passwords over their desk partitions. Other participants stated that they did not mind sharing their passwords with co-workers to get the work done. Another aspect of this culture was staff resistance to change which was considered an obstacle to any new technological related initiative including security. For instance, it was stated that in some applications many customizations have been undertaken, not to meet standards or best practice, but to match the old way of doing business that particular employees used to follow.

5.9.4 Technological Factors

In addition to the human and organisational factors presented previously, several technological factors have been identified in this study. These factors were directly related to the hardware and software infrastructures required to adopt e-Business:

1. *Complexity of emergent technology*: To meet changing demands and increase its computing power, the company has gone through a number of technological changes, from the time it was using a mainframe to the time when it became e-enabled and began running business over the internet. As the newly adopted technology can be characterised as fast and powerful, it also has an emergent property which is complexity. This increase in complexity was a result of the increase in the number of components and the interactions of these technologies. On

one hand, this increased their functionality and made them capable of performing additional and convenient tasks. On the other hand, increased complexity has a negative impact on security. As complexity of applications increases the complexity of security-related tasks such as requirement specifications and testing increase, which in turn increases the probability of missing some security requirements and having security holes. The effect of complexity of security has been observed in our case study. Participants argued that when the number of computers grew and became connected to the internet, things became more complicated from a security point of view. Also, it was stated that as the technology advanced in the company more security requirements were needed. Moreover, with the adoption of e-Business and the move from legacy systems to client-servers architecture, the company witnessed an increase in the number of security threats. Participants argued that the old system was less complex and access was very restricted, but in the new one new security threats such as network penetration, internet viruses and online fraud started to appear.

2. *Complexity of security and its tools*: This is another issue which has been observed during investigating the company approach to addressing online fraud. First, the fraud monitoring process depended on: collecting information from many parties, including acquirer bank, e-payment provider, and the internet booking engine; filtering this information to detect any suspicious transaction; and sending the information to other parties, including credit card section, e-ticketing and airport stations, to take further action. This complex network of interactions made the process of monitoring and preventing online fraud difficult because any defect in any link of this chain of interaction could lead to a situation in which processes fail. For instance, the fraud monitoring agent could miss a suspicious transaction and as a result of that the airport station would not be notified to check credit card holder information, then a fraudster would be able to use a ticket which had been purchased using a credit card which could be stolen; in this case the company would be liable to cover such a case of online fraud. The second notable issue was related to the usability of the fraud monitoring system which was based on generating daily lists of online transactions with their details. A dedicated employee was required to sit in front of a computer screen from 9am-5pm to filter and check these details to

see if there were any suspicious cases, and then inform the other parties. According to participants, this system was good when there were few transactions a day, but when the number of transactions started to increase dramatically, the monitoring process became awkward and increased the possibility of human error, which led to many transactions being missed. It was also notable that further conditions, such as screen size, internet speed, and reliability of the connection, made the process uncomfortable to use and frustrating. As this system was based on a human agent, another design flaw noticed was related to the fact that nobody worked on the system during the weekend, which increased the chances of online fraud going undetected.

3. *Accessibility versus Protection*: Conflict between these system properties has been observed and has implications for security. The study showed that in many systems the level of protection was required to be reduced in order to ensure accessibility of the services running on these systems. At the network level, participants stated that many security threats were coming from the open ports in the network which they could not block because many of their services were using these ports; if these were blocked it would affect their service availability. Similarly, in the fraud monitoring system, it was stated that the level of security control has been adjusted to make a balance between security and availability; unfortunately, this allowed a number of fraud cases to happen. This problem is possibly related to two interrelated issues which represent an example of the development of duality discussed previously. First, many applications have been developed with more focus on functionality and convenience than on security. Second, as the applications have been designed to run over the internet which was historically designed without security in mind; they have inherited its insecure properties, which causes conflict between fundamental properties (e.g. accessibility) and security, which was added at a later stage. This technology problem put the company in a situation in which it was required to make a trade-off between security and availability.
4. *Security of third party products*: the company depended on large number of vendors and third party products. Participants considered this product- based approach provided a less complex and cost effective way for adopting e-Business. However, it has a number of security implications. Although some participants argued that

they were not sure how much attention the providers pay to security, it seemed that for many participants the idea that products come secure from the providers was taken for granted. Unfortunately, this is often not the case; off-the-shelf products have always been vulnerable to diverse security breaches. Even products of large vendors are suffering from continued vulnerabilities.[6] Usually there is a gap between the time when a vulnerability is discovered and the time when a patch is created and deployed to fix it. This gives the attacker a window of opportunity to exploit this vulnerability and harm the infected systems. Another issue with third party products was the lack of compatibility, which could create security gaps. Participants argued security gaps could emerge when there was no compatibility between applications. They believed that limited integration between third party products ended the company with isolated islands and increased the chance of missing security as the whole picture was not clear.

5.9.5 Legal Factors

Factors affecting e-Business security which are related to the role of government and the current legal framework were grouped into one category, labelled as legal factors. Three legal factors have been identified in the context of this study:

1. *Absence of Effective Government Role:* From the study it became apparent that the government was not meeting the expectations of the different security stakeholders. When participants were asked about the current role of the government toward e-Business security there was a common agreement that the government is still lagging behind in this matter. Participants argued that the government should have a stake in e-Business security. For instance they suggested that it should build community e-Business awareness, which was considered as a prerequisite for building citizens' trust in the digital environment. On the other hand, they believed that the government should be the umbrella that regulates and controls this new trend. As e-Business involves different parties such as merchants, banks, and customers, participants argued the government should ensure secure integration between these parties and compel them to adopt good security practices. It was also

[6] A quick look at US-CERT Vulnerability Notes shows a list of daily security vulnerabilities which were founded in many commercial products. This can be found at http://www.kb.cert.org/vuls/bypublished

stated that government should contribute in providing security guidance for companies willing to adopt e-Business and help them to see a comprehensive picture about security.

2. *Legal Uncertainty*: the use of some security solutions that could contribute to improve security infrastructure has been affected by the legal uncertainty surrounding these solutions. This issue arose during discussion of the company B2B and online procurement process, in which there was difficulty fully utilising this mode of e-Business, as it is stated that such transactions require a signed agreement in order to authorise payments. When asked why the company does not use digital signatures as an alternative for the paper approval method, it was argued that the legal department was not comfortable using a digital signature because it was not yet properly tested in the country's courts. Despite the existence of the digital signature law, the lack of a precedent to see how the court deals with digital signature-related cases creates uncertainty, which has made the company reluctant to use such a security solution in their Business to Business transitions.
3. *Lack of Security Legal Setup*: Lack of a legal setup to protect both customers and businesses in the digital environment was another factor which had implications for e-Business security. Participants stated that there were no legal requirements for conducing e-Business in the country. Additionally, it was stated that nobody checks whether or not companies are capable of conducting e-Business from a security point of view, which left the matter subject to the companies' self-judgments. On the business side, participants believed that the current legal framework did not cover some important aspects of e-Business security such as the public key infrastructure and digital certificate authorities. On the citizen side, participants argued that the current legal setup does not encourage customers to use e-Business because it does not include data protection and credit card laws.

5.9.6 Factors related to Business Partners

Working with partners gives e-Business organisations the opportunity to focus more on their core business. However, working with partners might have a number of security implications which need to be carefully considered to provide a trustworthy e-Business environment. As one of the external stakeholders' groups, several business partners were

identified and their security implications were explored. These included organisations such as the oneworld alliance, and technology service providers. Factors which emerged in this category were related to the effects of the pressure of meeting business partners' requirements and the implications of outsourcing:

1. *External Stakeholder Requirements & Looming Deadlines*: As discussed previously, joining the international airlines alliance was a turning point in the history of the company. However, it was not an easy job because the company was required to undertake massive changes to meet the alliance's technological requirements. The company signed the alliance invitation in October 2005 and was given less than two years to fulfil its requirements to be able officially to join the alliance in 2007. This represented a challenge and created pressure on the company which did not want to miss the chance. More than six major projects which were launched pertained to updating the company's IT, financial and administrative systems to conform with those operated by the alliance's members. To cope with the time pressure, priority was given to the functionality and performance aspects as these could have a quick and tangible impact on the business. On the other hand, security was considered as an obstacle which could slow down the new transformations and e-Business adoption process. When asked about the reason why security was not given that much attention at the beginning of the adoption process, one of the participants stated that there was a very short time to accomplish all the required changes and they had to follow shortcuts to meet the deadline. Other participants stated that the company started with limited security and then tried to improve it. It was also stated that during the implementation of the internet booking system there was no time and they had to buy an e-payment gateway as soon as possible. It seemed that paying no attention to security or leaving it to be added at a later stage was one of the shortcuts taken to cope with the time pressure, which was the result of external stakeholder requirements.
2. *Outsourcing to Providers*: Another external factor affecting e-Business security in the company was outsourcing to technology services providers. Many of the company's e-Business applications were outsourced to third party providers. For instance, the website, the internet booking engine and payment gateway were hosted externally. Unfortunately, security was not part of the decision to outsource e-

Business applications, which was evident in the case of selecting an e-payment service provider who provided limited security measures; as a result the company started to suffer from online fraud. The study showed that the company decided to go for outsourcing without proper planning or enough knowledge about the implications of outsourcing. Some participants argued that outsourcing was the trend in the airline industry and, since many companies adopted this approach, these participants did not see any problem in following this approach. Other participants stated that outsourcing e-Business applications required agreement with the third party on the security of such a system, but the problem was that the company did not have enough knowledge about the requirements of selling over the internet, which led security to be overlooked. No evidence has been found to show that the decision for outsourcing was made after consideration of the possible security risks associated with such solution.

It is worth noting that these factors are interrelated and affect each other as well as e-Business security as a whole. The effects of and the interrelationships between these factors were synthesised and are discussed in relation to the relevant literature in Chapter 8.

5.10 Summary

This chapter has provided a detailed analysis that fulfilled the part of this study inquiry concerned with *how* security is perceived and addressed in the context of e-Business organisation. It started by exploring how e-Business emerged in this unit of analysis and how security was addressed during the transformation process. This has been achieved by exploring and investigating different aspects such as security functions within the organisational structure, security requirements process and how the company tried to protect its e-Business.

The analysis was facilitated by the use of interpretive stakeholder analysis, which led to identifying four groups of internal stakeholders. Internal stakeholders' security perceptions and interactions within an e-Business environment were explored, which in turn assisted in developing better understanding of how e-Business security was addressed in this study.

By analysing the company's approach to dealing with e-Business security and its implications the researcher was able to identify a set of socio-technical factors which influenced the company's particular security approach. These factors provided an explanatory and comprehensive framework for understanding e-Business security in the context of an e-Business organisation in Jordan.

While the analysis in this chapter has e-Business organisation and its internal stakeholders as its primary focus, it has built on and extended analysis from the first unit of analysis which explored the role of technology providers. Its findings were in line with the initial findings as they highlighted the role of other stakeholders who were found to have a significant role in the security of an e-Business environment. For instance, the analysis showed that outsourcing to technology providers influenced the way security was perceived and addressed in the e-Business organisation. It also showed that the absence of effective government role negatively affected how the e-Business organisation addressed security, which in turn could affect another group of stakeholders represented by the customers.

In both of the previous units of analysis, customers and government emerged as important stakeholders with security roles and requirements that need further investigation. The customer side of the security problem is explored in Chapter 6 and the security role of the government is explored in Chapter 7.

Chapter 6 : Analysing Customers' Side of e-Business Security

Customers have emerged in the previous two units of analysis as important stakeholders who affect and are affected by the security of an e-Business environment. Customers were found to indirectly interact and also influence technology providers through their direct interaction with e-Business organisations who normally fulfil their requirements through requesting new services and products from technology providers. Several aspects and issues related to this particular stakeholder were observed in the previous analysis. In the providers' study, issues such as lack of e-Business culture and distrust of technology have emerged. Other important issues were related to security awareness and the findings suggested that customers' security awareness can positively affect the security of e-Business products and services, as this awareness could create pressure on technology providers to pay more attention to security in their products and services so that customers can use them with greater confidence. In the second unit of analysis, customer satisfaction emerged as an important incentive for e-Business organisations. Yet its findings also suggested that the customers' culture and distrust were discouraging them from conducting transactions over the internet. Moreover, lack of effective security communication between e-Business organisations and their customers was observed as a factor heightening customer security concerns.

As the previous analysis provided initial insights into the customer's side of the problem, it is very important to explore these emergent security issues in a more direct and in-depth manner through an additional unit of analysis which has the customer as its primary focus.

Thus, this chapter aims to explore security issues surrounding online customers who are important e-Business stakeholders. Many studies have shown that Internet users in general and e-Commerce customers in particular are concerned about security and privacy over the internet (Pain et al., 2007). In a developing country such as Jordan, companies have started to conduct online business activities. However, surveys show that customers' concerns about security issues are the major obstacle for diffusion of e-Business in the country (Alsmadi, S., 2002; Khasawneh et al., 2009). In contrast to these previous studies, this

study provides a deeper insight into the customers' perspective of the problem and aims to answer the question of how customers perceive security of the electronic environment and its potential for conducting commercial transitions. To what extent people are aware about their online security and how they perceive online risks are important questions in increasing our understanding of the problem of e-Business security. Understanding the customers' social and psychological characteristics could open the door to designing better socio-technical security measures. Thus, the specific aim for this study is as follows:

To explore how customers' perceptions, awareness, education and expectations affect e-Business security in the context of the study.

To fulfill the aim of this research this study attempts to answer the following questions:

1. How do customers perceive security of the electronic environment and its potential for conducting financial transactions?
2. How does customers' security knowledge affect their online security behaviour?
3. How do customers perceive responsibility toward e-Business security and what do they expect other stakeholders to do?

Based on the above, it is the goal of this study to find out how security can be elevated to increase trustworthiness of the e-Business environment.

6.1 Customers' Unit of Analysis and Findings

Several themes have emerged from the data analysis using the thematic framework analysis technique guided by the inductive coding process described in the first unit of analysis. After close reading of part of the qualitative data, initial themes have emerged through identifying segments (descriptive elements) from text highlighting perceptions, actions and issues related to the study research questions. As the analysis process proceeded, the initial themes were refined and supported by additional descriptive accounts. The final list of themes was grouped and categorised into three conceptual categories as shown in Table 6.1. Each interview was given a symbolic name to ensure anonymity and ease of access. This symbolic name consists of the letter C (indicating that the interview is a customers/citizen interview) followed by a number from 1-27. Sampling issues and data

collection related to this unit of analysis have been discussed in the research design presented in Chapter 3.

Table 6.1: Themes and categories which emerged from the customers' case study.

Category	Emerged Themes	Location in text
Security Perceptions	Security & privacy needs	C1,C2,C3,C5,C9,C10,C11,C12,C13, C14,C15,C16,C17,C18,C20,C23,C26
	Limitations of technical security solutions	C1,C2,C3,C5,C11,C19,C22,C23,C26
	Building trust with the supplier	C3,C5,C6,C7,C9,C11,C12,C13,C15, C16,C19,C22,C23,C25
	Perceived capability to protect online security	C1,C2,C3,C4,C5,C6,C7,C11,C12,C13, C15,C16,C18,C20,C22,C23,C26,C27
	Threats of the online environment	C1,C2,C4,C5,C6,C9,C10,C11,C13,C14 ,C15,C16,C17,C18,C20,C22,C23,C25, C26
Security Awareness	Limited awareness of good security practices	C2,C3,C4,C7,C8,C9,C10,C14,C16,C17 ,C20,C21,C23,C25
	Limited awareness of companies' mechanism to provide online security	C1,C2,C3,C4,C5,C7,C8,C9,C10,C13, C14,C16,C17,C19,C20,C21,C23,C25, C26,C27
Security Expectations	Customer responsibility	C14,C19,C23
	e-Business organisation responsibility	C2,C5,C6,C7,C8,C9,C10,C11,C12,C13 ,C14,C15,C16,C17,C18,C19,C20,C21, C22,C23,C25,C26, C27
	Government responsibility	C1,C2,C4,C5,C6,C7,C8,C9,C10,C11, C12,C13,C14, C15,C16,C18,C19,C20, C22,C23,C25,C26,C27

As shown above, 10 main conceptual themes emerged which were grouped under three main conceptual categories: Security Perceptions, Security Awareness and Security Expectation. Details of these findings are presented in the following sections.

6.2 Customers' Security Perceptions

To explore how customers view the online environment, a number of overarching topics were discussed with participants, aiming to explore their perceptions and concerns about the potential of e-Business in the country. Since customers are usually involved in the customer-to-business side of e-Business, most of the questions focused on this particular mode of online business.

There was strong evidence grounded in the data supporting the claim that customers value the notion of e-Business. However, other evidence showed that they have perceptions and serious security concerns which prevented them from performing commercial transactions over the internet. From the analysis carried out five themes involving perceptions and

concerns emerged; they are: security and privacy needs; limitation of technical solutions; building trust with supplier; self capability to protect online security; and threats within the online environment. The five conceptual themes depicting customers' security perceptions are discussed in details below.

6.2.1 Security & privacy needs

Customers' perceived need for security and privacy emerged as a natural requirement that needs to be fulfilled to encourage them to use e-Business with confidence. The values of security and privacy were appreciated and requested by most of the study participants who argued that these two aspects are important for them and that they would feel safe if these aspects were ensured in an e-Business environment. For instance, it was argued that "*security is important and it should exist to protect users from any malicious internet sites*" and, regarding privacy, one participant believed that "*everybody should have privacy on the internet...it is important requirement*".

Privacy needs were expressed in terms such as "*having control over personal information*", "*not being monitored over the internet*" or "*to have your own online space*". Some participants saw no difference between online and offline privacy and believed that privacy should be ensured in both cyber and physical worlds. They argued that access to or use of personal information should be based on the permission of the person who owns this information. Additionally, violation of online privacy was considered unwanted and uncomfortable, for instance it was stated that:

"It is annoying when you feel that somebody is trying to read your personal information or trying to see what you are doing over the internet".

In addition, participants emphasised the need to have a secure online environment to protect customers. They believed without security it is difficult to use the internet with confidence. Moreover, it was argued that security is important for building trust with the other side of the transaction. Security was understood by them as a means to "*protect the end users from online threats and to prevent any attempt of malicious act*".

Notably, many participants were able to distinguish between privacy and security as two different constructs. Few used the term privacy to define security or the opposite. This highlights the point that e-Business systems should pay attention to both security and

privacy aspects, as in some implementations ensuring one does not imply ensuring the other.

6.2.2 Limitations of technical security solutions

Another point revealed in this study was related to the customers' perception about the security of internet technologies and the ability of technical security solutions such as personal anti-viruses, firewalls and anti-spyware to provide them with an adequate level of security. Many of them believed that internet technologies, which are the backbone for e-Business, have their limitations and are not without deficiencies which could lead to many security implications:

"In any electronic system there are deficiencies. Companies tried to protect their systems; however, there are people who can break these systems. Who builds these systems knows everything about them and could use this knowledge to break them".

Based on that, they argued that their level of trust in these technologies is limited. This perception was also fostered by their belief in the imperfection of the humankind who developed these applications:

"...Technology provides us with many benefits; speed, convenience...etc. But still technology may contain faults because it is designed by humans who usually make mistakes".

Another participant raised a similar point and argued that *"no absolute trust, it [the internet technology] is human made and humans are not perfect so how will you trust it"*. Anther issue which emerged was related to the security of the close source software in which it was argued that no one except the developers knows what is hidden inside the software. For instance, one participant, who believed that nothing is completely secure or safe, argued that the widely-used Microsoft Windows operating system is full of vulnerabilities which cause security breaches.

In addition to the perceived security limitations of internet technologies, many participants saw that available security technical controls are unable to prevent security threats completely. They mentioned many cases in which their computers were infected by viruses or hacked despite the fact that they were using all the possible security solutions. This problem was understood by some participants as a result of the rapid advancement of

internet-related technology which is not matched with similar advancement in security, thus giving a window of opportunity for an attacker to exploit security weakness before they get fixed:

"The personal security applications are incapable to protect you completely. Technology is evolving very quickly and once a new application is deployed, hackers figures out how to break it".

In summary, this leads us to conclude that technological solutions have their limitations; moreover, that technology and security are moving at two different speeds, in that security is lagging behind, thereby leaving technology vulnerable all the time.

6.2.3 Building trust with supplier

Participants raised the issue of establishing trust with the other part of an e-Business transaction. Some of them argued that online transactions are intangible and it is difficult to trust the other side of the transaction. Accordingly, they considered face-to-face transaction more reliable as they could physically verify the identity and assess the trustworthiness of the other side. In one instance, it was argued that this issue has its roots in the offline world where people used to carefully assess and establish trust relationships because of many past incidents which created a lack of trust culture.

On the other hand, there were many participants who considered B2C e-Business potentially very useful. This group included participants who showed their willingness to try it and others who had already started using it. While those customers were concerned about security and trust, it was necessary to explore what affects their decision to transact with any particular online merchant and what role security plays in their decision-making process. From the study it became apparent that customers depended on a number of concerns to help them to assess the security and trustworthiness of online merchants. Some of the findings suggested that the existence of security measures and information about them in the merchant's online portal were used by some participants as trust and security assurance concerns:

"...Before I use their e-commerce systems I like to read how much security they have and what is going to be if something happened".

"I try to check if it is registered with 3B which is online company which registers any site which accept visa card as a payment method. Also you should check their digital certificate".

However, the majority depended on other concerns which were not necessarily related to the real security of the website or the merchant's actual security practices. For instance, it was stated that *"if the design of the website is nice it could encourage the customer to buy from it"*. Another participant stated that the site appearance gives him/her the feeling how much effort the company had put into the website and this affected his/her decision to buy from the site. Others talked about the quality of the service and how much information is available on the website about the products they intended to buy. One participant mentioned that s/he could phone the company to make sure it really existed. Two methods were frequently cited by participants to assess online trustworthiness. First, company reputation, which was expressed in terms such as the *"online company should be well-known"*, *"it should have brand name"* and *"it should be recognised"*. Some participants also believed that if the company is new in the market, it is unlikely to succeed over the internet, as first it needs to build a name in the offline world. The second frequently-cited concern was the recommendation of friends and people who tried to transact online with a particular merchant. Many stated that they referred to somebody who already used the website they intended to buy from, to check if that person experienced any problems, and based on that they decide whether to transact with it or not:

"I try to ask people who tried the website I'm planning to use. Sometime I look to its policy to see the terms and conditions, however, I depend more the others experience to decide whether to transact with this website or not".

Although customers seemed concerned about security, these findings suggest that they appear to be unaware of many security controls and features (third party certificates, encryption, privacy policy, etc.) which online merchants usually use to increase customer trust and ensure security. Consequently, they depend on other factors such as reputation and recommendations of others to get some kind of online assurance.

6.2.4 Self-capability to protect online security

When asked about their capability to ensure their online security, participants seemed not confident about this matter and perceived themselves as lacking competence in protecting their security. They discussed many factors which they believed contributed to this lack of competence. For some of them, there were factors which are out of the online customers' control. In addition to the technical limitations discussed in the previous section, they

stressed that the online environment is not controlled and is full of unexpected events that could affect their online security. For example, one of the participants discussed how a popup windows or some links in one website could redirect you to another website that you did not intend to visit, which could be a malicious one. They also thought that whatever they did to ensure security, there are always *"bad guys"* equipped with superior knowledge and skills who can violate their online security:

"No I cannot protect my security, you can not be aware of everything, and there are other people who are smarter than you and they could try to deceive you over the internet".

"...but still there are hackers who are very expert I don't know everything about their tricks".

Other participants related their incapability to ensure their online security to their lack of security knowledge. This has been expressed in terms such as *"don't know everything to protect online security"* and *"my security knowledge is limited"*. In other instances it was argued that customers cannot protect their online security because they are not educated from the security point of view:

"I don't have enough expertise to protect my online security. Everything I know about that is just small personal effort. We don't have any course or training about that".

Also it seemed that many were convinced that only experts could gain the knowledge that can help them to protect their security. Another point which emerged from discussing this topic was related to the role of the other stakeholders in relation to customers' online security. For instance, it was stated that if the other parties involved in e-Business fail to secure their sides, it will not be enough to secure the customer side. Another aspect of stakeholders which emerged was related to the role of some parties such as government and regulatory bodies in helping customers to protect their online security. These stakeholder points were followed by questions in order to further explore the customers' expectations and perceptions regarding the security role of other stakeholders in an e-Business context. Findings of this part are presented in section 6.4.

6.2.5 Threats of the online environment

When asked about buying or selling over the internet, customers' responses showed that the idea was in principle acceptable, moreover, they were able to identify several potential

advantages for e-Business such as saving time, effort and money. However, exploring their actual online behaviour gave the indication that many of them would use the internet for many activities except those involving financial transactions. The study results showed that this reluctance to engage in real e-Business transaction was partially due to customers' fear of being subject to the various security threats associated with the internet environment. Table 6.2 shows the list of customers' perceived threats of the online environment.

Table 6.2: List of perceived security threats associated with e-Business.

Threats	Description
Online Fraud/Deception	A threat of losing money in transaction includes dishonest party.
Hacking	Unauthorised access to customer's computers and information.
Impersonation	Pretending known legitimate online merchant in order to deceive customers.
E-mail Theft	Unauthorised access to customer e-mail account
Credit Card Theft	Gaining access to customer's credit card or its information by unauthorised party.
Malicious Software	Harmful applications such as viruses, spyware, and Trojan horses.
Personal Information Abuse	Using customer's information in a way that could lead to unwanted consequences.

Most of the study participants had been using the internet for more than 6 years and for different online activities. Despite the fact that participants believed the internet is useful, most of them were unwilling to provide sensitive information over the internet, as they perceived the internet as an open and insecure environment which could expose their information to different security risks. The following quote demonstrates this perception:

"*I don't like to give personal information over the internet...I like to keep my personal data secret...I believe that the internet is vulnerable and this could make my personal information subject to risk*".

The study also revealed that this perception was not only a general fear of the internet environment, but was based on an awareness of specific security threats, as shown in Table 6.2, that customers fear when carrying online commercial transactions. In addition to the common security threats such as *hacking attempts*, *spying* and *virus attacks*, it was also argued that there are possibilities for online impersonation, and deception. One participant argued that *"anybody could create a website and claim that it is representing a company*".

Others expressed their fears of transacting with dishonest merchants who might not deliver items, send faulty ones or charge more that the price shown in the website.

These perceptions were not always based on a customer's personal experience with the merchant, but also on stories of other people who tried to buy products over the internet:

"...It is fearful. I heard many stories, in one, a person bought shoes from a website where the price on the internet was 70$, but when he received the bank statement he found that 200$ have been deducted from his account. So how you can guarantee that this will not happened for me".

From the analysis it became clear that both personal experience with online security threats and the recommendations/anecdotes of other people who have had unpleasant experiences with e-Business services have played an important role in shaping customers perceptions of risk. This online risk perception formed a barrier which made customers reluctant to provide personal information online in general or participant in e-Business transactions in particular.

6.3 Customers Security Awareness

While the above findings showed that customers were concerned about security, it suggested that they might lack the necessary security knowledge which can help them to increase their online security. Two main themes emerged under this conceptual category. The first theme was related to awareness of security skills and practices which aim to protect customers' online security and reduce the number of threats that they might face. The second theme focused on awareness of the common security mechanisms that online companies implement in their e-Business portal to provide customers with the required security assurance.

6.3.1 Limited awareness of good security practices

To explore customer's awareness of good security practices, participants were asked a number of questions covering aspects such as security features in their personal computers, security applications they use and procedures they follow to ensure their online security. Many of them stated they always make sure they have anti-virus software installed in their machines to protect their online security. Few stated that they had a personal firewall, anti-spyware or web filter which could increase the level of protection that a normal anti-virus

can provide. Regarding good email practices, many of them stated that they delete emails which have been received from unknown sources as these emails either contains ads or viruses. This assumption was made by some customers after experiencing security breaches as a result of opening emails or attachments from unknown sources. Others stated that their curiosity led them to open and read such emails and in many cases this exposed them to serious security risk:

"Yes I experienced one of these cases in which I received an e-mail saying that I won 100,000 $ and I just need to send 700$ to get the prize. Then I felt that somebody try to fool me and I didn't reply to that email".

In another instance, a customer was a victim of such fraudulent emails. These examples show that such security threats cannot be prevented using anti-virus or firewalls, but by cautiousness which need to be improved through increasing people's awareness of security.

Exploring how customers choose and use their password gave more insight into awareness of good security practices. Using passwords as an authentication mechanism is common over the internet and many online companies provide customers with a user name and password to provide secure access to their accounts. Two aspects of password use were explored. Participants were asked whether they use different passwords for different accounts or not, and how they usually chose their passwords. The analysis showed that most of them were using one password for many online accounts. This bad practice could put customer's personal information at risk because if this single password is revealed, all his/her accounts can be easily compromised:

"I used to have one password, but after some e-mails theft incidents I started to use different passwords for each account".

While these participants seemed unaware of the important of this practice, they argued that choosing one password for different accounts is convenient especially for recalling the password. The study also revealed that most of the respondents had an incorrect belief about strong passwords. Exploring how they choose their passwords showed that they tended to use very personal information such as persons' names, car names and phone numbers.

"I use one password and I choose something special to me like my university ID or phone number...like that".

"I have one password...I use numbers or names which have special things in my mind".

Few participants stated that they used passwords which include a mix of letters, number and special characters, or that they avoid using personal information as a password as it is easy to guess.

The study revealed that customers never received any training or course related to security. Despite the fact that the educational system in the study context covered computer literacy aspects, participants argued that it did not cover anything related to information security, which left them with limited awareness based on personal effort. From the study it became apparent that customers' awareness of good security practices was very limited and this made them subject to many security risks, especially the threats which are difficult to prevent technically, such as phishing or password-related threats. While they depended on some technical security solutions to protect them from threats such as viruses and malware, there are other threats which cannot be prevented by these technical measures. For example, having an anti-viruses or firewall will not protect the customer from bogus emails requesting him to submit his bank account details and pretending that this is needed by the bank to update his records. Protecting customers from such threats requires increasing their security knowledge and awareness of these threats and how they need to react to these threats.

6.3.2 Limited awareness of companies' mechanisms to provide online security

As discussed in section 6.2.3, customers depend on a number of antecedents to assess online merchants' security and trustworthiness, which were not necessarily related to the actual security practices of the online merchants. This raised the question whether customers are really aware of common security mechanisms (digital certificates, privacy policy, secure communication and encryption) usually implemented in e-Business portals, as this awareness could help them to avoid any false feeling of security and enable them to increase the number of antecedents that could eliminate their security concerns.

Table 6.3: Terms related to common web security mechanisms.

Term	Brief Description
Digital Certificate	Issued by trusted certificate authority and used to identify the identity of the online merchant.
Encryption	Several techniques used to convert data in cipher data which is only readable by authorised parties.
Secure Website	Website which has security features such as digital certificate, privacy policy and apply encryption.
Privacy Policy	Placed on the merchant website and informed the customer how his personal information is going to be used.
SSL	Secure Socket Layer protocol, used to provide confidential and not tampered-with communication between customers and online merchant.
HTTPS	Usually appears at the URL address bar to indicate the website will encrypt the customer information and send it over SSL channel.

To explore customers' awareness of these common approaches for providing online security and increasing trust perceptions, participants were presented with a list of terms related to these security mechanisms and were asked to comment on them. These terms are shown in Table 6.3. Very few participants were able to provide a brief description similar to the one shown in the above table. Some provided short and unclear descriptions; for instance, one participant stated that the secure web site is the "*safe website*" without being able to clarify how a website can be safe or secure. Another described a privacy policy as a "*document in the website which talks about privacy*". However, the majority had no idea what these terms related to.

E-Business organisations depend on these security measures to provide online security and trust assurance to their customers. Arguably, these security controls could improve their security assessments in two significant ways. First, customers' concerns might be alleviated when they are made aware of these security controls, and furthermore their existence might increase their perception that a merchant is secure and trustworthy. Second, the researcher argues that this knowledge empowers customers to have real control which can be used alongside their anecdotal recommendations and common sense perceptions to assess online merchant security.

6.4 Customers' Security Expectations

As discussed previously, the study showed that customers were concerned about security and privacy which were considered by them as important needs and requirements for a trustworthy e-Business environment. Therefore, it was necessary to understand and explore

how responsibility toward e-Business security is perceived by customers in the study context, and how they perceive the role of other stakeholders in relation to this matter. Three different expectations have emerged depicting customers' perceptions about the responsibilities of several security stakeholders represented by the customers themselves, e-Business organisations, and the government.

6.4.1 Customer responsibility

The analysis revealed that customers felt less responsible for ensuring their online security. Little evidence was found to claim that customers perceived themselves as responsible for adopting measures to increase their security while transacting over the internet. The majority deposited this responsibility on other stakeholders such as the companies doing online business and the government which represented the role of the state in the study context. They perceived themselves as users who just receive online services without any control over these services or the infrastructure underlying them. Few participants believed that customers must share part of this responsibility. For instance, one participant argued that security "*is personal responsibility and everybody should take care of what he is doing on the internet*". In another instance, it was argued that security is the customer's responsibility and "*he should be aware of the internet risks*". However, this was less evident compared to the common perception in which participants believed that businesses and government are mainly responsible for e-Business security.

6.4.2 e-Business organisation responsibility

Companies doing online business have emerged in this study as important stakeholders in the security of the e-Business environment. Participants believed that the primary responsibility for ensuring e-Business security lies with online companies. From the customer's perspective this responsibility includes three main tasks: protecting customers' information held by these companies; providing the necessary measures to secure their e-Business applications and infrastructures; and contributing to building customer trust and security awareness.

Participants argued that online merchants should be responsible for protecting customers' information and ensuring that this information will not be used in any way that could harm them. They emphasised the importance of credibility and transparency of the online

companies. Accordingly, they argued that online merchants should have clear and transparent procedures regarding how customers' information is going to be used and protected. The existence of such procedures was considered paramount:

"*The company which will receive and process my information is responsible to protect my information. It should have an expert to prevent unauthorised access to my sensitive information. Before I use their e-commerce systems I like to read how much security they have and what is going to be if something happed*".

They also emphasised that companies should secure their e-Business portals using all possible technologies, procedures and professional expertise. In order to increase customers trust, they argued that companies need to work more on the security of their websites and it was suggested that these companies should hire security experts and consult with professional security providers to ensure an adequate level of protection. Additionally, participants highlighted the importance of communication with customers in order to understand their security needs:

"*Online companies should have good security systems. Also their credibility should be very high and they should communicate with the customers to understand their needs and requirements. All this will build the customer trust in these companies*".

The study showed that customers were not well-informed about the security of available online services that local companies offered. Participants argued that these companies do not put much effort into advertising and marketing their e-Business services and how secure they are. Moreover, they argued that online merchants need to communicate the security of their online services effectively to the customers:

"*They should secure their websites and they should increase advertisement and promoting the security of their websites. For example they can talk in the newspapers about how much they are secure to encourage people to use their websites*".

It was believed that communicating security to customers will serve two purposes. First, it will increase the customers' trust in e-Business organisations as having security and will provide them with more assurance that their information will be protected. Second, it will contribute to build customers' security knowledge and awareness as they will be informed about how online companies secure their e-services.

6.4.3 Government responsibility

Government and regulatory bodies were viewed as other important stakeholders who must have a stake in the security and trustworthiness of the e-Business environment. In general the study revealed that customers expect more effort from the government toward the security of the e-Business environment, which they believed should be part of its responsibility towards its citizens. When asked who should be responsible for ensuring a secure electronic environment, many participants argued that this should be part of government responsibility which is required to protect citizens and companies transacting over the internet. As they seemed unsatisfied with the current situation which does not meet their expectations, they suggested many actions that the government could undertake to increase trustworthiness of e-Business in the country. For instance, involving government in controlling and organising the e-Business environment was expected to have a positive impact on the level of trust in e-Business transactions. It was argued that this could provide some assurance that the process is not left to the judgment of the individuals or companies involved in these transactions. Moreover, it was believed that the government could act as an independent authority that parties involved in e-Business transactions could refer to in case of any conflict. Accordingly, this could encourage people to transact online and increase the chance that e-Business will succeed in the country:

"*The Government should be responsible for providing secure e-environment; if you look to the west and why e-commerce succeeded there, it is because the governments are involved in everything... The government should be the guarantor for anything that could occur online*".

Government responsibility for the security of the e-Business environment was seen by customers to include a number of tasks. Many instances showed that customers wanted e-Business activities to be controlled and monitored by the government. This was expressed in terms such as "*monitoring online companies*", "*controlling online environment*" and "*protecting online customers' rights*". Also it was suggested that the government should make sure that these companies are registered and it should check the capability of these companies to conduct online business in a secure manner:

"*The government can have a big role in this, if any company is going to run business over the internet, this should be through the government approval. This includes what the company is going*

to sell and how it is going to collect/return money to the customers. All these are important to protect online customers".

Additionally, participants emphasised the need for a clear legal framework for e-Business activities. Therefore, they argued that government should be more active in the process of enacting laws to protect parties involved in e-Business transactions. Both proactive and reactive actions were requested by participants. In addition to the need for regulatory acts to protect online customers' rights and to ensure that online merchants are capable of conducting secure online business, participants argued that government should react to any illegal online activities which could harm businesses or customers, therefore, there should be a digital crime law to punish any one who commit such illegal actions:

"*The government should be responsible for the internet security and it should put rules, regulations, and laws for online business... There should be a specific authority in charge for security and there should be a clear law to punish for illegal online activities*".

Although Jordan was one of the early countries in the region to pass legislation to regulate online contracting, its electronic transaction law 80 0f 2001 was not sufficient to provide customers with the necessary rules to protect them from the risks associated with the online environment. In contracts with many developed countries[7], Jordan did not provide clear rules and regulations for businesses to consider before setting up an online business. This could explain why participants expected that the government should have a more significant role in regulating e-Business in a way that would protect their rights.

Furthermore, it was expected that the government could contribute to reducing online threats by applying some security measures on the internet infrastructure such as "*filtering internet traffic to ensure it is free from viruses*" and "*restrict access to malicious websites*". Given the fact that this infrastructure became owned by private telecommunication companies[8], it would not be easy for the government to perform such actions. However, it may force telecommunications companies to apply these security measures which raise the security bar in the digital environment. This can be realised by passing regulations which force

[7] See for example http://www.out-law.com/page-424 for a list for rules that companies in the UK need to consider before establishing selling over the internet.

[8] In 1996 the government started the privatization program in order to reduce the public sector stake in and rebalance many economic sectors. As a result of this program the telecommunication sector was completely privatised.

these companies to adopt the required controls in order to ensure secure online environments and by regulating the internet infrastructure by security standards that could provide stability and trustworthiness.

The last role that customers believed that the government needs to consider was building citizens' security awareness. While the government was required to encourage the adoption of e-Business, it was argued that it is responsible for equipping citizens with the knowledge and skills to use e-Business applications in a secure manner. Customers emphasised that the educational system did not give attention to raise citizens' security awareness:

"*At the academic level this subject are not given enough attention and students graduate without enough knowledge about security and privacy issues*".

In the light of these findings, the current role of the government will be explored in more detail in the next chapter, which will be the final unit of analysis in the research. The researcher will attempt to gain more insight in the government role and other security legal aspects by investigating current government efforts towards the security of e-Business in the context of the study and the implications of these efforts.

6.5 Summary

This chapter has focused on the customers' side of e-Business security and analysed how their perceptions, awareness, education and expectations influence security of e-Business in the context of the study. On the basis of the findings, it can be argued that many customer related aspects need to be considered in order to elevate e-Business security. These aspects include customer perceptions and concerns, customer security knowledge and interaction with stakeholders, including government and business organisations.

Although the findings suggested that customers appreciate the potential benefits of e-Business, they showed that security concerns acted as a barrier to full engagement in online transactions. Several factors have been found contributing to these security concerns; these included the fear of being subject to various online threats, vulnerability of Internet technologies, limitations of technical security solutions, and the intangible nature of e-Business transactions. The findings also suggested that the customers' lack of security-related knowledge negatively affected their ability to take rational security decisions while they conduct transactions over the internet, which increases the chance of being subject to

security threats. Also, the analysis showed customer security perceptions and security knowledge were influenced by interaction with the government and online companies and how much those stakeholders communicate security to the customers. Regarding online companies, the findings suggested that their responsibility toward security includes three main tasks: protecting customers' information held by these companies; providing the necessary measures to secure their e-Business applications and infrastructures; and contributing to building customers' trust and security awareness. On the other hand, customers seemed less satisfied with the current role of the government toward the security of e-Business. Accordingly they suggested several actions, including regulating e-Business, securing the national ICT infrastructure, and building public security awareness.

In the light of these findings and the ones from the previous units of analysis, the next chapter will analyse the current role of government in the security of e-Business in the context of this study.

Chapter 7 : Analysing the Role of Government in e-Business Security

This chapter presents the fourth and final unit of analysis in this research and explores the role of government and regulatory bodies in relation to the security of the e-Business environment in the context of the study. In the study's initial framework of inquiry government was identified as an important stakeholder whose effect could span a wide range of stakeholders and security aspects. The framework speculates that government involvement in e-Business security will affect several dimensions, particularly technical, organisational and legal. Through the previous three units of analysis, which explored technology providers, e-Business organisations, and customers/citizens, the need for an effective government role emerged as one of the important themes. Thus, the aim of this chapter is to shed light on the current role of the government in the security of e-Business and on what has been done to meet the relevant stakeholders' expectations. This has been achieved by reviewing government documents and conducting a number of interviews with government officials involved in a number of e-Business activities in the country.

Although the adoption of e-Business in the context of this study is still in the early stages, a number of observations show that this adoption is increasing dramatically. The move into the online environment is notable according to the Global Information Technology Report (GITR), which shows that the country was very successful in leveraging ICT which in turn reflects on its economic efficiency and service provision (Word Economic Forum, 2009). The country's profile in this report is in line with the findings of the previous three units of analysis, which suggest that the government is still lagging behind when compared with the businesses and the individual's readiness to participate in the online environment. While the GITR is one of the few public reports which provide a valuable source of data about the diffusion of ICT in many countries, including Jordan, it also raises awareness of the importance of ICT diffusion, identifies its enabling factors and stresses the responsibilities of different stakeholders, including governments, businesses, and individuals. Yet, limited information security aspects are covered by the GITR. For instance, it does not assess the government's contribution in securing national ICT infrastructure or building public

security awareness, as this study's findings stressed. This leaves a gap which needs to be filled by exploring how policymakers at the national level tackle security during the transition into the digital environment.

Accordingly, this particular unit of analysis aims to answer the following questions:

What is the current role of government regarding e-Business security in the context of the study? And how it can be an effective partner in the problem area?

From the previous analysis it has become apparent that there is a common agreement between the relevant stakeholders that the government should put more effort into meeting their requirements and expectations which in turn would reflect on the security and trustworthiness of e-Business in the country. In the light of these stakeholders' requirements and expectations, it is the goal of this study to investigate the following:

1. How does government address e-Business security in the country's legal framework?
2. How is e-Business security addressed in the current national e-Commerce strategy proposed by government?
    a. How does government perceive security and what aspects does it intend to address?
    b. What are the current government's efforts and plans to build security awareness for both business and citizens?
    c. What are the current government's efforts and plans to secure e-Business infrastructures?

Section 7.1 analyses e-Business security aspects with the current legal framework. It investigates the electronic transaction law and its implication for the security of e-Business in the country. Section 7.2 analyses government policies, strategies and action plans in relation to e-Business security. Section 7.3 provides a summary and the implications of the findings.

7.1 E-Business Security in the Current Legal Framework

Recognising the importance of legislation that facilitates e-Business transactions in the country, Jordan was one of the first countries in the region to pass a special law for online transactions. The temporary law is called Electronic Transactions Law (ETL) No 85. of year 2001 and represents the single legal reference that can be applied to e-Business transactions (ETL, 2001). Instead of amending existing legislation to recognise online transactions, this special law was introduced to be applicable to any transactions that may include electronic processing, transmitting and storing of data. The law attempts to regulate a number of e-Business aspects including electronic contracts, recodes, messages and signature. Also, it provides a set of articles related to electronic transfer of funds and authenticity of electronic documents. Moreover, it represents the first step in the effort to prevent some sorts of cybercrime.

While the ETL is the only legal reference that can be found in the county in relation to e-Business transactions, it does not provide a comprehensive set of legislation that can ensure security and trustworthiness of the online environment. A close look at this law shows that it has a number of limitations which make it inadequate to provide the required legal setup. A review of the law's provisions and discussion of its limitations are presented in section 7.1.1 and 7.1.2.

7.1.1 Overview of the Electronic Transaction Law (ETL)

According to article (3) of the ETL, the law was introduced to enable electronic means of conducting transactions. These transactions include both governmental and commercial online transactions. It consists of 7 chapters and 41 articles which for the purpose of conducting secure e-Business can be considered in terms of the following four areas:

1. Electronic documents including records, contracts and messages.
2. Electronic transfer of funds.
3. Electronic signatures and digital certificates.
4. Penalties for some kinds of online abuse.

First, regarding the use of any electronic document, it is important that the law acknowledges the legal power of the different forms of electronic document and considers them acceptable sources of evidence that cannot be denied just because they are conducted by electronic means. Indeed, according to article (7/a) of ETL "*the electronic records, contracts, messages, and signatures shall be considered to produce the same legal consequences resulting from the written documents and signatures in accordance with the provisions of the Laws in force in terms of being binding to the parties concerned or in terms of fitness thereof as an evidential weight*". Similarly, article (8/a) of the law sets the conditions for considering the electronic record to have the same legal effect as the original form, which mainly focus on availability, accessibility and integrity of the data contained in the digital record as well as identification of the originator.

Second, at the core of e-Business is the notion of electronic transfer of funds. ETL stipulates a number of provisions that aim to facilitate e-payment, which is considered an important component in e-Business infrastructure. For instance, article (25) recognises the electronic transfer of funds as an acceptable payment method. Only two general conditions have been set on financial institutes providing e-payment services. First, they should comply with other relevant laws such as the Central Bank of Jordan law and the Banks law, as well as regulations and instructions that the Central Bank issues to regulate e-payment in the country. The second condition obliges these institutions to ensure security in terms of security of the services provided to clients and maintaining banking confidentiality.

Third, the law defines "Electronic Signature" as the only mechanism which provides security and acceptability of the "Electronic Record" which is defined under the ETL as "*a record, contract or data message generated, sent, received or stored by electronic means*". It stipulates that the electronic record is valid and deemed secure from a legal point of view only if it is signed by a secure electronic signature which is generated during the validity period of its digital certificate, which needs to be obtained from an accredited certificates authority. This implies that the existence of a Public Key Infrastructure (PKI) is required for implementing this law.

Finally, in terms of secure e-Business, it is important that there is some means of preventing related abuse. In Jordan, the law stipulates provisions related to some cybercrimes which mainly focus on illegal use of digital certificates. Both imprisonment

and fines have been introduced as penalties for illegal online acts such as the creation of security certificates for fraudulent purposes or unlawful activities. Penalties have also been introduced for organisations involved in the process of securing electronic records. For instance article (37) stipulates that "*any entity engaged in the practice of securing documents which submits false information in a registration application, or discloses confidential information of any of its clients, or violates the regulations and instructions issued pursuant to this Law documents shall be subject to a fine of no less than (5000) five thousand dinars*". In article (38) the law goes farther and introduces punishment for any act which is considered a crime committed by electronic means.

7.1.2 Analysing ETL in Relation to e-Business Security

Although the ETL is considered an important step for increasing the adoption of e-Business in the country by providing a suitable legal framework for such activities, several issues related to e-Business in general and security in particular are not covered in this law. From the analysis it becomes apparent that it has many limitations which render the current legal situation inadequate for providing a secure and trustworthy e-Business environment which should address all the relevant stakeholders' needs and concerns.

The first major drawback which can be noticed in this law is that it is not obligatory. This means it is applicable only if the parties participating in a particular e-Business transaction agree to apply it. This is clear in article (5/a) which states "*unless a provision in this Law states otherwise, the provisions of this Law shall apply to the transactions on which the parties thereto agree to implement the transactions thereof through electronic means*". In the same context, article (5/b) requires a new agreement between the parties for every new transaction. According to Al-Ibraheem and Tahat (2006) this is because the law is based on the model law of the United Nations Commission on International Trade Law (UNCITRAL) [9] which requires explicit consent from the parties that are going to perform transactions by electronic means. Whilst this provides some sort of flexibility to the parties transacting online, it means that the law might not be implemented at all and this means that it will not fulfil its goal of regulating e-Business in the country.

[9] The United Nations Commission on International Trade Law (UNCITRAL) www.uncitral.org

An additional reason which makes a large part of this law ineffective is the lack of regulations and instructions on how to implement and enforce some of its provisions. For instance, the validity of the electronic signature is linked, under this law, to the validity of the digital certificate which needs to be issued by a competent and licensed certificate authority. According to article (40/b) the Cabinet will issue the necessary regulations for implementing the provision related to "*the procedure for issuing security certificates, the authority competent to do such and the application fees*". Unfortunately, these regulations have not been issued until now (ESCWA, 2009). Absence of these regulations makes it impossible to establish such fundamental security infrastructure in the country. Other missing regulations are related to the security of electronic transfer of funds which, according to article (29), should be issued by the Central Bank of Jordan which is responsible for maintaining and ensuring the safety of the banking environment in Jordan. This lack of supportive regulations, especially the ones related to security of online transactions, hinders the establishment of secure e-Business infrastructure and increases the legal uncertainty which in turn hinders building trust in e-Business at both business and citizen levels.

In relation to punishment for online illegal activities, The ETL covers very limited aspects of cybercrime, mainly addressing the illegal use of digital certificates. Additionally, it introduced a penalty of up to one year's imprisonment for any illegal act which is conducted online. This implies that the law does not distinguish between the wide range of cybercrimes which can differ in terms of type, intention and severity. Under the current law there is no difference between simple computer penetration targeting any machine over the internet which can be committed by a teenager and organised denial of service attack targeting large e-Business portals in the country. Looking at the nature and diversity of cybercrime, it can be argued that these provisions fail to recognise the wide range of real risks associated with e-Business environments and fail to deal with each type of these crimes according to its nature and impact.

In addition to the above limitations, several important security aspects are not covered under the current legal framework. These mainly include online privacy and data protection, online customer protection, and security of e-Business infrastructure.

Despite the fact that the Jordanian constitution seems to respects citizens' privacy in the physical world, there is no equivalent treatment for online privacy. For instance, internet cafés, which are very popular in the country, are requested by law to collect personal data from the internet users. This data includes identifiable information and internet use records must be disclosed if the government so requests:

"*In March 2008, Jordan began increasing restrictions on the country's Internet cafés. Under the pretext of maintaining security, Internet cafés were installed with cameras to monitor users, and Internet café owners were required to register the IP number of the café, the users' personal data, the time of use and the data of Web sites explored*" (OpenNet, 2009, p. 3).

According to the ESCWA (2007) the lack of data protection laws and non-existence of disclosure control mechanisms are the major cause of privacy problem in many countries including Jordan:

"*While most advanced countries have devised laws that protect privacy and data, all ESCWA member countries still lack standards and regulations to protect personal privacy and data, with the exception of general laws that are applied in certain cases*" (ESCWA, 2007, p. 38).

Furthermore, there is a clear lack of laws and regulations to protect the rights of customers engaging in e-Business transactions which represents a serious obstacle for building customer trust in such forms of transaction. Consumer protection includes many issues such as product liability, privacy rights, fraud and misrepresentation (ESCWA, 2007). Unfortunately, these issues are not covered under the current legal framework which can contribute to an increase in legal uncertainty in e-Business environment of the country.

In relation to the security of e-Business infrastructures, which may include security guidelines, standards, procedures and techniques that the commercial sector should follow in order to ensure security, there is a clear absence of legislation that covers such issues. For instance, there are no regulations for establishing online stores in general (Al-Ibrameem and Tahat, 2006) or for securing them in particular.

Based on the issues discussed above, it can be argued that the current legal framework is inadequate to provide a trustworthy e-Business environment and has failed to address several security aspects, including enforcement, supportive regulations for establishing security infrastructure, cybercrimes, privacy and online customer protection. While these

issues are among the main concerns of a wide range of stakeholders, a comprehensive legal framework to cover them is much needed for today's complex e-Business environment.

7.2 Security in the light of the National e-Commerce Strategy

It is notable that the government has recognised the potential benefits that ICT diffusion in general and e-Business adoption in particular can bring to the country. In the course of the last 10 years, it has been working hard to increase the country's electronic readiness to get the most from the information society. Consequently, ICT and its related applications became one of the hot topics on the government's agenda and several initiatives were launched to realise its benefits. This is also reflected in government policies which started to include a dedicated part for ICT. In 2007 the government policy for ICT and postal sectors called for more efforts to encourage local companies to offer e-services especially e-Commerce services (ICT-Policy, 2007). In reaction to the recommendations of this policy, the Ministry of Information and Communications Technology (MoICT), in cooperation with other governmental bodies and stakeholders, introduced the National e-Commerce Strategy for the period from 2008 to 2012 in order to provide the necessary framework for implementing those recommendations (MoICT, 2008). As this research calls for integrating security as an important component of e-Business adoption strategy, the aim here is to explore how and to what extent the government addresses security in the national e-Commerce strategy.

7.2.1 Overview of the National E-Commerce Strategy

The national e-Commerce strategy represents the government plan for developing e-Commerce in Jordan. Under this strategy, e-Commerce is defined as "*transactions between consumers and businesses or between businesses associated with the development or trade of goods and services over telecommunications or broadcast network*" which implies that this strategy is intended to cover all e-Business modes, including business to customer, business to business, and internal business automation. The strategy was drawn up based on the Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis, which was carried out between July and October 2007 to assess the current state of e-Business in the country. Consequently, five major factors were identified as reasons why e-Commerce had not taken

off in Jordan. These are: the lack of e-payment systems; the lack of supportive legislation; the lack of e-Commerce awareness; unaffordable broadband access and PCs; and arbitrary tax changes. Therefore, the strategy's vision, goals and objectives have been set with the intention of overcoming these impediments and their related issues.

Therefore, the vision of the strategy was to make Jordan "a leading e-commerce centre in the region through the exploitation of its information technology capacity and the creativity of its people". In the light of this vision, four strategic goals along with a set of objectives associated with each of them were defined, as shown in Table 7.1.

Table 7.1: Goals and objectives of the national e-Commerce strategy (MoICT, 2008).

Strategic Goal	Related Objectives
1. To increase the wealth of the Jordanian people through the development and exploitation of e-commerce	▪ To create an environment that generates business opportunities particularly for young people. ▪ To create additional high value employment for Jordanians in knowledge based industries. ▪ To improve the efficiency of Jordanian business. ▪ To reduce factor prices.
2. By 2012, to be a regional leader for IT systems development, applications and services associated with e-commerce	▪ To expand the domestic and export markets for ICT products and services. ▪ To increase the gross revenue and gross value added by the sector. ▪ To increase tax revenues raised from the ICT sector. ▪ To improve Jordan's ability to attract skilled ICT professionals to come to or remain in the country. ▪ To increase the range of e-commerce products and services.
3. To be one of the leading countries in the region that uses e-commerce as a channel for selling goods and services to consumers.	▪ To increase the number of Jordanian retailers that sell online using e-commerce within Jordan, in the Arab region and worldwide. ▪ To stimulate retail e-commerce business start ups ▪ To improve consumers' access to goods and services sold by Jordanian retailers. ▪ To reduce the cost of goods and services for Jordanians. ▪ To extend the range of goods and services available to Jordanians. ▪ To increase the volume of Jordanian domestic retail business. ▪ To extend the reach of Jordanian retail businesses across the Arab region. ▪ To increase the profitability of Jordanian retail businesses.
4. To be one of the leading countries in the region that uses e-commerce as a channel for domestic and international business to business collaboration and trade	▪ To increase the number of businesses that use e-commerce for business to business trading within Jordan, in the Arab region and worldwide. ▪ To stimulate wholesale e-commerce business start ups. ▪ To maximise Jordanian company participation in global supply chains that use business to business e-commerce as their channel. ▪ To increase the efficiency of supply chains operating in Jordan. ▪ To extend the range of goods and services available to Jordanian companies. ▪ To extend the reach of Jordanian companies in existing international markets and reach new international markets. ▪ To increase the efficiency of individual companies in the procurement of goods and services.

In order to implement this strategy and to fulfil its goals and objectives a wide range of enabling factors were identified; these factors were associated with enabling actions with potential owners and possible stakeholders. These enabling factors and their description are shown in Table 7.2.

Table 7.2: Enablers of the National E-commerce Strategy (MoICT, 2008).

Enablers	Description
The Law	Provide an effective legal framework for the development of e-commerce including the validity of digital signatures, consumer protection, cybercrime and various changes to the e-transaction law.
Security	General awareness of the need for information and personal security amongst companies that trade electronically.
Electronic payments	Fully operational payment gateway and associated banking services for use with internet and mobile phone payments.
Tax	Develop systems and processes for tax audit of electronic records, tax simplification.
Awareness	General awareness throughout society, awareness of lawyers and judges, of SMEs, of government officials, an d of banking staff
Skills	Develop commercial and technical e-commerce skills amongst SMEs and ICT firms, commercial and legal e-commerce skills amongst lawyers, judges and tax officials.
Customs	Introduce rapid customs clearance and associated customs IT systems.
Employment	Provide employment opportunities that meet the aspirations of the educated young.
The IT sector	Develop capacity in e-commerce, e-commerce software and services for fixed and mobile sectors; promotion of the sector skills.
Availability and use of ICT infrastructure and services	Competitive supply of broadband, widespread adoption of broadband; improvement in the affordability of ICT; introduction of 3G mobile services; competition and diversity in international telecommunications.
Logistics and transport infrastructure	Develop warehousing and packing facilities; remove impediments for the development of air and land freight hubs.
Catalogues and content	Establish capacity in e-commerce content development.
Finance and investment	Improve links between investors and entrepreneurs.
Government	Advance the use of e-procurement in government.

The government delegated the governance authority of the strategy to a National E-Commerce Governing Body comprising ministers whose interests affect the implementation of the strategy. Under this governing body, a National E-commerce Council was established to be responsible for implementing the strategy. This council comprised ministry representatives and other representatives of stakeholders, including the Central Bank, Jordan Information Technology Association, Chamber of Commerce, and Chamber of Industry.

7.2.3 Analysing e-Business security aspects within the strategy

The above overview of the government's strategy to develop e-Business shows that the strategy was intended to cover a wide range of areas including legislation, local ICT industry, infrastructure, and financial services. Moreover, its actions targeted a wide range of stakeholders including customers and service providers as well as government departments so that all the relevant stakeholders' requirements could be fulfilled. The important question then is: How and to what extent is security addressed within this strategy? Is it comprehensive and sufficient to fulfil the requirements?

Here the researcher presents the answer for the above question by exploring three points:

i. What was covered by the strategy in terms of actions and mechanisms to ensure security.

ii. Perception of Security in government strategy.

iii. The deficiencies of the government plans and actions in providing security.

These three points are discussed in the following subsections.

What has been addressed

The strategy clearly acknowledged that the lack of trust in e-Business related activities is among the important barriers that need to be overcome. The strategy related this lack of trust directly to the lack of an adequate legal framework and lack of security awareness among potential online merchants. Also, it speculated that the level of trust would increase as society became more familiar with e-Business transactions.

In connection with these barriers the strategy focused on two points which mainly touch on the security of e-Business. First, it set a number of actions to address some of the limitations of the current legal framework, especially in relation to customer protection and the security of e-transactions. As discussed in section 7.1.2, the Electronic Transaction Law (ETL) was not able to provide a complete set of provisions to ensure online security. This was also acknowledged by the government's strategy which included in its action plan the need to amend the current ETL to cover issues such as confidentiality of e-transactions, preventing spamming, dispute resolution, and ensuring effective enforcement measures.

Additionally, the action plan included promulgating three new laws; Cyber Crime Law, Consumer Protection Law, and a law to establish Credit Bureau facilities in Jordan. The second point that the strategy focused on and considered important for leveraging security of e-Business was increasing awareness amongst potential online companies about the need for information security measures. Therefore the action plan included publishing security guidelines for online companies and the target was to achieve 90% of online merchants conforming to these guidelines two years from the issuing data which has been left unspecified.

To this extent security has been addressed in the national e-commerce strategy and it seems that the government felt that its proposed action plan was appropriate for assuring e-Business security and eliminating the relevant stakeholders' concerns. Although it addressed very important issues, especially in relation to the legislation that promotes a secure online environment, the strategy has a number of interrelated deficiencies which render it inefficient in providing the holistic security which is necessary to ensure trustworthiness of the e-Business environment. These deficiencies can be observed at each of the strategic, governance and action levels of the strategy. These deficiencies and their possible implications are discussed below.

Security deficiencies of the national e-Commerce strategy

Looking at the strategy's goals and objectives presented above gives the indication that securing the e-Business environment was not perceived as a strategic goal that the government intended to fulfil. Instead, security was perceived as a hurdle which could simply be removed by giving security guidelines to online companies and passing a certificate authority law and other relevant laws and regulations. This narrow understanding of the role of security and its implications could be the reason for the strategy not having a comprehensive and a systematic approach to addressing wider security aspects. Not having security as a strategic goal can increase the chance that it will be overlooked in many areas associated with the implementation of the strategy. This can be observed in many parts of the proposed action plan, such as ICT infrastructure, logistics and transportation, skills, and awareness. For instance, in the ICT infrastructure section of the action plan, it was stated that MoICT in collaboration with telecommunication operators and local ISPs would ensure the availability of the ICT infrastructure necessary for e-Business services; therefore, it

included a number of actions that cover this part. Unfortunately, none of these actions was related to the security of ICT infrastructure in the country, which gives clear indication that security was missing from this part. Consequently, this narrow understanding of the role of security could affect the other goals that the strategy aimed to achieve. For example, in the second and fourth goals of the strategy, the government wishes to make Jordan a regional leader for IT services and a strong competitor in the digital economy. If security is not integrated into the process of achieving these goals and if it is not considered as a competitive advantage, these goals are unlikely to be achieved, because security of IT services is an important factor for companies who want to provide their customers with a high quality, reliable service. Many developed world companies are off-shoring part of their business to developing countries and relying heavily on their ICT infrastructure to communicate with customers and provide services. A lack of security could lead to Jordan being excluded from the benefits of such opportunities, which would have a negative impact on the strategy's goals.

Another deficiency, which also can be linked to not perceiving security from a strategic point of view, is the lack of governance framework for information security. Although the government is the owner of this strategy it does not seem to want to take a larger part of the responsibility toward ensuring security in general and e-Business security in particular. The strategy clearly stated that "*as an implementer of e-commerce strategy, however, Government's roles and responsibilities are limited. This strategy lays down objectives for Government to meet in areas such as the law associated with e-commerce, taxation and customs. The strategy also lays down objectives for the private sector to attain...As programme manager, Government can facilitate, promote, propose, recommend and sometimes fund, but seldom command or require action by the private sector*". Revisiting the results of the previous units of analysis shows that other stakeholders, especially customers, were suggesting that the government should be more involved in this matter and it should have a clear role and responsibilities for securing an e-Business environment which goes beyond the legal role. However, it seems that the government is depositing this responsibility on the private sector without even taking responsibility for forcing the private sector to do that. Lack of such governance framework at the national level implies that the policy makers are not aware of the wider implications that security may have on the digital economy, including issues such missed business opportunities, unprotected ICT

infrastructure, and customer distrust. The existence of a clear security role and the responsibilities that need to be exercised by the government are necessary to ensure government commitment towards securing the e-Business environment, which was considered by many stakeholders to be a natural part of the government's responsibility towards its people.

At the action level, the strategy action plan only focused on limited security aspects. The first security action that the strategy proposed was related to reforming the legal framework to cover issues such as establishing security certificate authorities, cybercrime, and consumer protection. The second proposed action was intended to promote security of e-Business websites through proposing set of guidelines to build the security awareness of online traders. On the other hand, other important security aspects were overlooked; these include building public security awareness and securing e-Business infrastructure.

Despite the fact that the action plan proposed many actions to raise e-Business awareness in different sectors and among a wide range of stakeholders, these actions only focused on the benefits of e-Business and none of them emphasised the need to build information security awareness especially among stakeholders such as customers, judges, lawyers, and government officials. The strategy only recognised the importance of this aspect on the online merchants' side; therefore, it suggested publishing guidelines to raise their security awareness. Building citizens' security awareness could contribute to increasing their levels of confidence and equipping them with skills that might help in protecting their online security, thereby elevating trust in e-Business. Failing to do that, the strategy failed to fulfil the government ICT policy which stated that "*Government requires that users (both residential and small business) be supported by the provision of advice on the safe use of the Internet and the protection of children, in order to promote consumer confidence in the use of ICT, while avoiding risks and protecting human rights. This function should be led by the MoICT and should include participation by other relevant public and private stakeholders*" (ICT Policy, 2007). One can argue that considering factors such as ICT skills, knowledge, and education in the strategy indirectly implies the necessity for having in place security practices to use and manage ICT. In fact this could be misleading and most of the time security aspects are overlooked, come as an afterthought, or are perceived from a purely technical dimension. Based on the above, it can be argued that the strategy

needs to recognise the importance of information security awareness at different levels of society as a starting point for cultivating a security culture, which in turn would contribute to enhancing the trustworthiness of e-Business as a whole.

At the infrastructure level, the government seems to want to invest heavily in providing citizens with physical ICT infrastructures without paying much attention to secure these infrastructures which are required by e-Business adopters. For instance, the strategy emphasised the availability and affordability of e-payment systems, broadband and wireless services, without requiring service providers such as ISPs and telecommunication companies to have the requirements of securing these services, which might increase the risk that security will be overlooked in these critical infrastructures. Lack of attention to security can also be observed at the strategy part which focused on the logistics and transport infrastructure necessary for e-Business activities. The government stressed that these components are essential to facilitate and increase the adoption of e-Business, but it overlooked security, which is an important factor in increasing adopters' confidence in the logistics and transport systems. Without security in these components, customers' orders are subject to many risks, including theft, replacement, damage, and even violation of customer privacy.

Regarding the protection of e-Business infrastructure, a similar point has been highlighted in the previous unit of analysis by interviewed customers, who argued that the government should contribute to the security of ICT infrastructure by ensuring the existence of security mechanisms which reduce potential threats of the Internet, which is the main medium for e-Business activities. This also applies to the delivery system which can be the source of many security threats.

7.3 Summary and implications

This chapter has attempted to describe and analyse the current role of the government in the security of e-Business. The analysis was guided by the study framework of inquiry to explore its role from different security dimensions and in relation to different stakeholders. The findings of this unit of analysis revealed that the government had a very narrow view of security and this had a number of implications for its plans and initiatives to promote an attractive e-Business climate. This first government attempt to address security was through

the Electronic Transaction Law (ETL) which included a number of provisions which were intended to provide a secure online environment. The empirical analysis shown in section (7.1.2) revealed that this law was inadequate to provide a trustworthy e-Business environment and failed to provide a mechanism to address several security issues which were among the main concerns of a wide range of stakeholders. These issues included online privacy and data protection, online customer protection, and security of e-Business infrastructure. Besides, the lack of supportive rules and regulations to implement and enforce some provisions in it, especially the ones relating to establishing certificate authorities, rendered a large part of it inactive and therefore unable to fulfil its goal. The National e-Commerce Strategy was introduced seven years later and represented an acknowledgment from the government that the existing legal framework hindered adoption of e-Business in the country as it did not cover the above issues. It attempted to overcome that by proposing a set of actions to reform the current legal setup to better facilitate e-Business. These actions included promulgating three new laws; Cyber Crime Law, Consumer Protection Law, and a law to establish Credit Bureau facilities in Jordan. Nevertheless, it failed to perceive security outside the legal dimension. Even when the government acknowledged the relation between security and citizens' trust in e-Business, its proposed action plan did not go beyond providing security guidelines to online companies, and the legal role was predominant. The analysis conducted in section (7.2.3) suggested that security was not viewed as an essential part of the strategy nor as a competitive advantage. Consequently, this reflected on its goals and objectives, which overlooked security. This ignorance of security at the strategic level combined with a narrow understanding of the multifaceted nature of e-Business security leads to major two implications. First, it has lead to a situation in which security has been overlooked in many areas at the implementation level of the strategy. This was notable in the action plan which covered areas such as stakeholders' awareness, ICT infrastructure, and logistics, but which lacked any plan to address security aspects associated with them. Such a lack of security in different e-Business areas could have negative consequences including customer distrust and discouraging investors as well as financial losses. Arguably, these economical implications could increase the risk of not achieving the strategy goals and objectives which were intended to develop e-Business and to create a competitive digital economy. Second, there was no national security governance framework to establish a set of roles and

responsibilities that the government and other relevant stakeholders need to exercise to ensure security of the e-Business environment. In such a situation it is difficult to know who is in charge of what, and security is left to the judgment of the individual parties involved in e-Business without any reasonable auditing or control mechanisms to ensure that they will follow acceptable security practices.

Although the government, including its policies and plans, seems serious about exploiting the potential benefits of e-Business in the country, overlooking security in its broad sense could jeopardise all its efforts to acquire those benefits. Based on the above, the study suggests that the government should recognise the full range of socio-technical implications that security/lack of security may have on the adoption of e-Business. This can be achieved by understanding the real security needs and concerns of the various stakeholders at the different e-Business stages. It then needs to align and integrate these requirements with its policy and plans. It also suggests that in order for the government to be an effective partner in developing a secure e-Business environment, it is not enough to limit its role to promulgating laws and regulations addressing security issues, but it should have a multifaceted role which might include, in addition to legislation, increasing security education and awareness, monitoring, ensuring compliance with security standards and regulations, and protecting the country's critical ICT infrastructure.

Chapter 8 : Synthesis, Discussion and Evaluation

This research has aimed at developing a conceptual framework for better understanding of the various issues surrounding security within an e-Business environment. To fulfil its aim, the thesis has defined an interpretive stakeholder approach in which concepts from a socio-technical perspective assist in constructing a framework of inquiry used to support the research design and outcomes. The interpretive stakeholder inquiry has been used to explore all the interested stakeholders and investigate their interrelationships and interactions in an e-Business security environment.

The aim of this chapter is to bring together the main findings, identifying their interrelationships and implications. Additionally, it provides an evaluation of the overall research process and ends with possible future research directions.

8.1 Discussion of the Main Findings and their Interrelationships

Absolute security could be unattainable (Audestad, 2005). However, many actions can be taken to raise the level of security in an e-Business environment. This research investigates how security can be incorporated to provide a trustworthy e-Business environment; it argues that identifying and understanding the different security stakeholders are important steps for knowing what actions need to be taken to increase security in a way that provides a trustworthy e-Business environment. From the stakeholders analysis employed in this research, several socio-technical factors influencing e-Business security have emerged (see figure 8.1). These factors contributed to the problem situation in which security was overlooked, came as an afterthought or, at the best, was approached technically. This section provides a discussion of the security factors emerging from the four units of analysis presented previously. It synthesises the relevant themes, identifies linkages between them, and positions them within existing knowledge. It provides an explanation of the factors involved and how they mesh together to provide the detailed explanation in Figure 8.1.

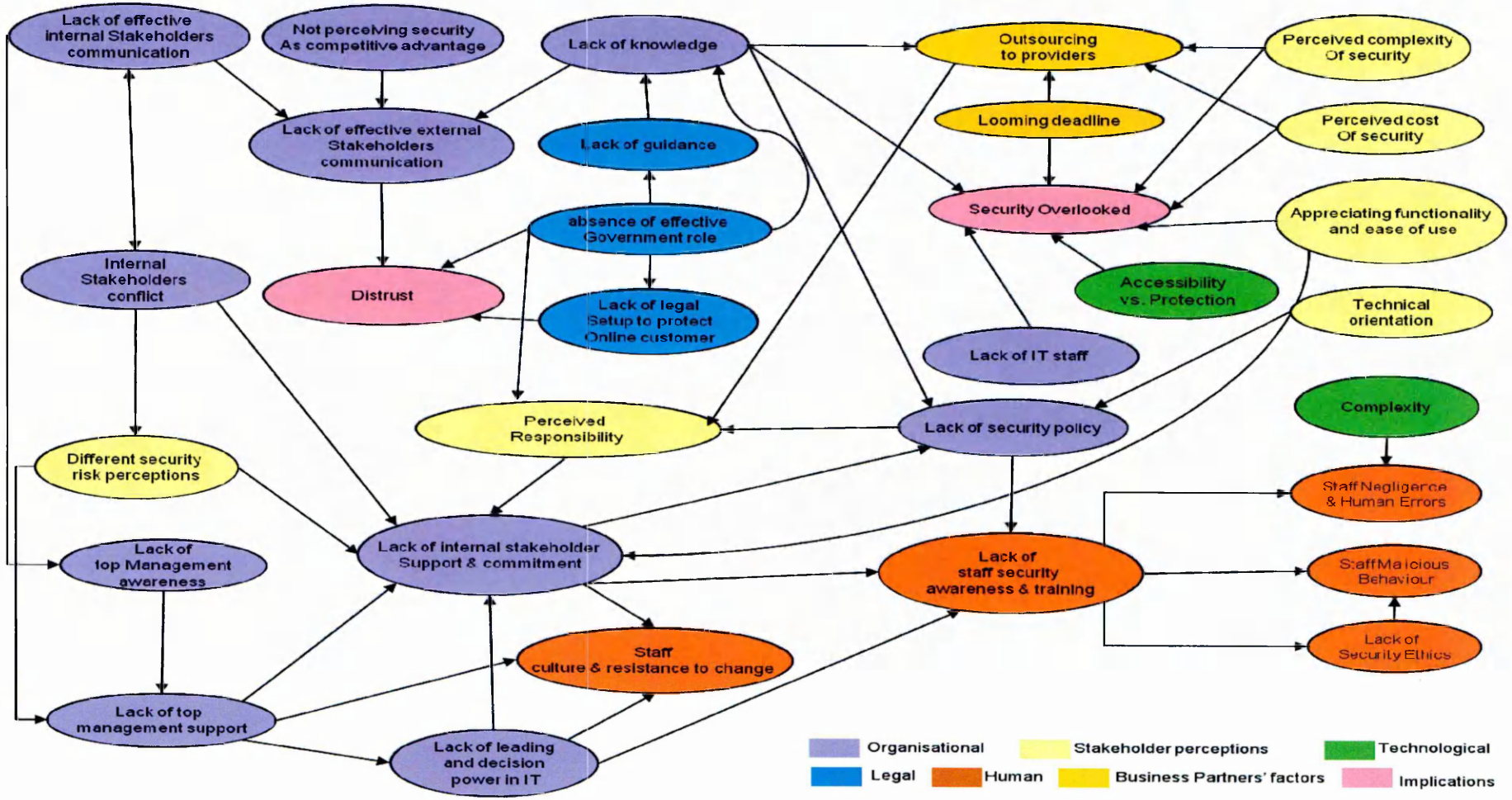

Figure 8.1: Socio-technical factors affecting the security of e-Business environments and their relationships.

8.1.1 Issues surrounding top management support to security

Within e-Business organisations, the study revealed that the involvement in and awareness of top management of e-Business security were very limited, as security was not part of the business strategy and the decision making process. For instance, top management was pushing towards adopting business-to-customer online services and fulfilling the business partners' technological requirements without giving any attention to security. However, when top management became informed about a serious security threat represented by online fraud, which led to financial losses, it showed a markedly increased interest and there was significant support for any solution that could solve this security issue. This illustrated how increasing top management awareness of both e-Business security and the implications of security breaches did increase its involvement and support for any security initiatives which otherwise might have been considered unnecessary. This result confirms Straub and Welke (1998) who argued that that the effectiveness of an organisation's information security approach is highly dependent on management awareness of information security and the wide range of actions that it can undertake to reduce information security risk.

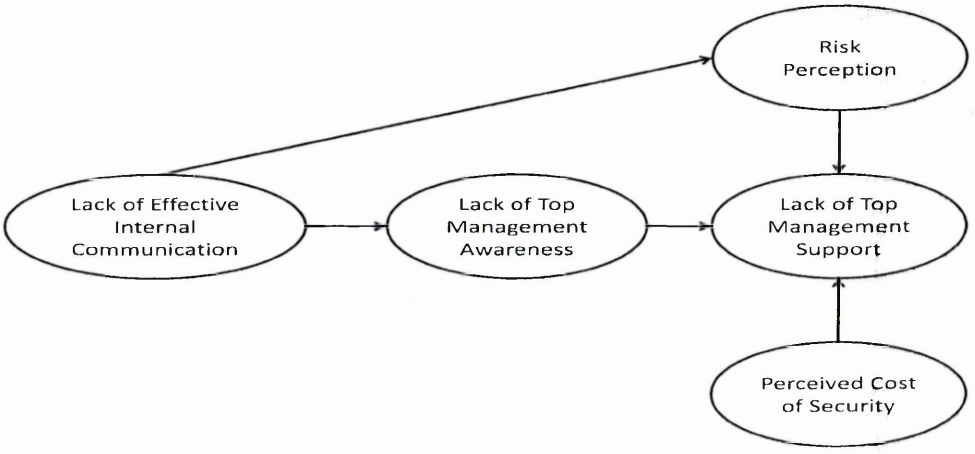

Figure 8.2: Factors affecting top management support for information security.

The impact of managers' awareness of information security on their actions towards information security has been investigated by Chio et al. (2008) who concluded that building an organisations' awareness should influence its security action and thus enhance the organisation's security performance. In fact, in the discussion of the limitations of their

findings, Chio et al. (2008) suggested that there should be other factors in addition to top management awareness. While our findings are in line with those findings, we also found that this support was constrained by the perceived cost of adding security and the perceived risk – especially the financial risk - associated with the area that needs to be protected. For instance, the analysis showed that if the amount of revenue generated from the area that needs to be protected is very low and the cost of adding security is relatively high, security is likely to be overlooked.

Another important factor the study revealed as significantly affecting top management's security awareness is the lack of effective internal stakeholder communication. Although some participants argued that it is the role of IT management to communicate security to the top management and increase their awareness regarding the various security risks associated with an e-Business environment, the study showed that limited security aspects were reported to top management. For instance, only the financial losses relating to fraud cases were reported; awareness of this particular threat explains their providing support to solve this issue. Moreover, investigating the organisational structure, roles and responsibilities showed that security incidents and potential security threats were not communicated to top management. Accordingly, it can be contended that the lack of effective internal communication and reporting impacts on top management's awareness of security. Other studies have explored the relationship between the lack of communication and information security incidents in organisations (Kraemer & Carayon 2006; Werlinger at al., 2009). Kraemer and Carayon (2006) in their study of 16 network administrators found that the lack of proper communication between network administrators had a negative effect on security. Moreover, Werlinger at al., (2009) discussed how ineffective interactions between security stakeholders could lead to vulnerabilities in organisations. While lack of effective communication has contributed adversely at the operational level as the above studies show, this study's findings suggest that it also negatively affects top management awareness and support. It also suggests a relationship between effective communication and risk perception; communicating more security-related information to top management can affect its risk perception by encouraging it to understand and consider additional security risks it might not have been aware before (Straub & Welke, 1998).

The importance of top management support for security in organisations has been highlighted by many researchers (Straub 1990; von Solm & von Solm, 2004) and it has recently been ranked as the top information security issue facing an organisation (Knapp et al., 2006). However, few studies provide a rich picture for the different factors affecting top management's support for security. Top management support and the new picture of relationships with the other factors discussed above are encapsulated in Figure 8.2.

8.1.2 Internal communication and its effect on risk perception and stakeholders' support of security

This study showed that the differences in stakeholders' perceptions of security risks were also because of the lack of effective internal communication between these stakeholders. Analysing stakeholders' security perceptions showed that the serious security threats perceived by the IT people were not necessarily understood or the same for the business people. Take for example the threats to the internal business environment such as employees' malicious behaviour or negligence, which were underestimated by most participants from non-IT departments. This confirms Flechais and Sasse (2009), who found that the lack of effective communication between those with more security knowledge and those with less security knowledge contributed to the existence of two different mindsets.

When participants from the IT department were asked why IT people did not try to communicate security to business people, it was stated that business people did not understand security or its importance, and they did not like it when IT people suggested something to them to improve security, as they considered this to be interference with their job. This also illustrates how the tensions between stakeholders might affect the company's security approach. It was also stated that the business people believed that the role of the IT department is technical and they have nothing to do with the business, which makes it difficult for the IT people to have a say in business. As Wang (2005) suggested, this represents an internal rivalry in information security which needs to be carefully managed to ensure a successful information security program.

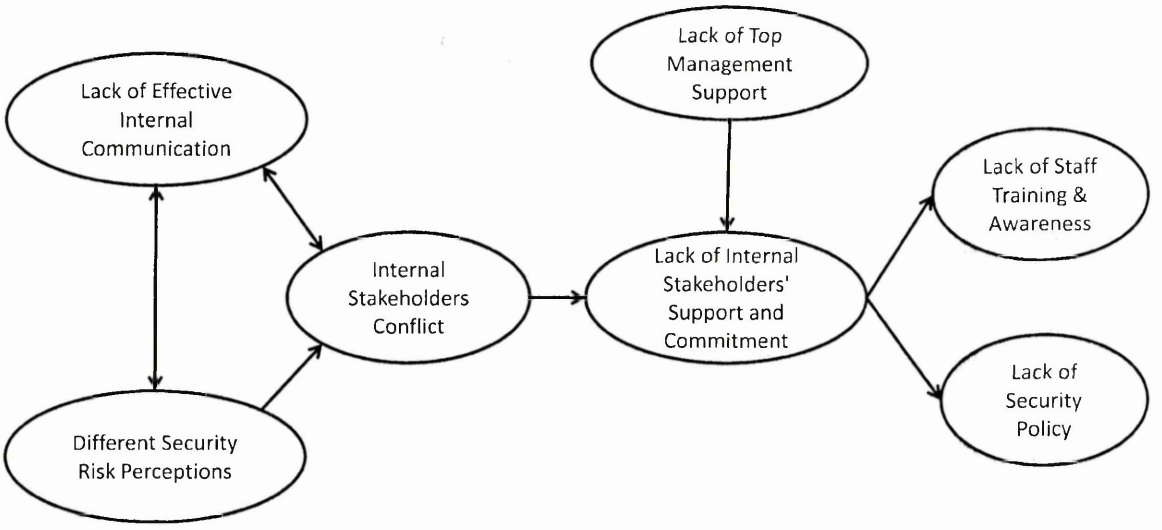

Figure 8.3: Communication, risk perception and internal stakeholders' support.

As shown in Figure 8.3, this lack of effective communication contributed to creating different security risk perceptions and conflict in stakeholders' interests. On the other hand, the conflicting interests of stakeholders made the stakeholders communication difficult, which is supported by other empirical evidence reported in Werlinger at al. (2009). Moreover, the internal stakeholders' conflict and the lack of top management support made it difficult to get internal stakeholders' commitment and support for security initiatives. For instance, staff security awareness training had been proposed by the IT department five years previously, but it did not find anybody to support it and it was stated that the human resource department and business management were busy and did not want to waste time with something they considered unimportant. Similarly, the lack of internal stakeholders' support and commitment delayed the implementation of security policy which was prepared as a draft by the IT department, but there was no support from the other departments.

8.1.3 External communication and its security implications

The issue of ineffective security communication between internal stakeholders was found to influence the way e-Business organisations communicated with external stakeholders represented by its customers. Although communication with customers through marketing channels was considered by the study's participants as a way of building trust, security was not part of this communication. While security is considered one of the important

components for building online trust (Furnell & Karweni, 1999; Tsiakis & Sthephanides, 2005), online companies need to ensure that security requirements are an essential part of the customer relationship strategy, which implies that e-Business infrastructures need to be secure and their security needs to be communicated to the customers. The analysis of the respondents' answers and reviewing the company website showed that security was not promoted to the customers in a marketing means through the use of logos, trusted third party seals, or brochures. Excluding security from communication with customers was due to three reasons (see Figure 8.4). Firstly, some participants who were involved in marketing e-Business did not perceive security as a competitive advantage and thought that customers did not need to know about security. For other participants, it was the first time they had encountered such a thing, hence, their lack of knowledge contributed to not promoting security to build customer trust. Finally, the lack of effective communication with the IT department and the lack of collaboration with marketing contributed to this situation; when IT participants were asked about promoting security to the customers, their answer was "*we don't have direct communication with the customers and the marketing department decides what to tell the customers*". This contradicts Shankar et al.'s (2002) advice that website characteristics, including security, and company communication with customers are among the important antecedents of building online trust.

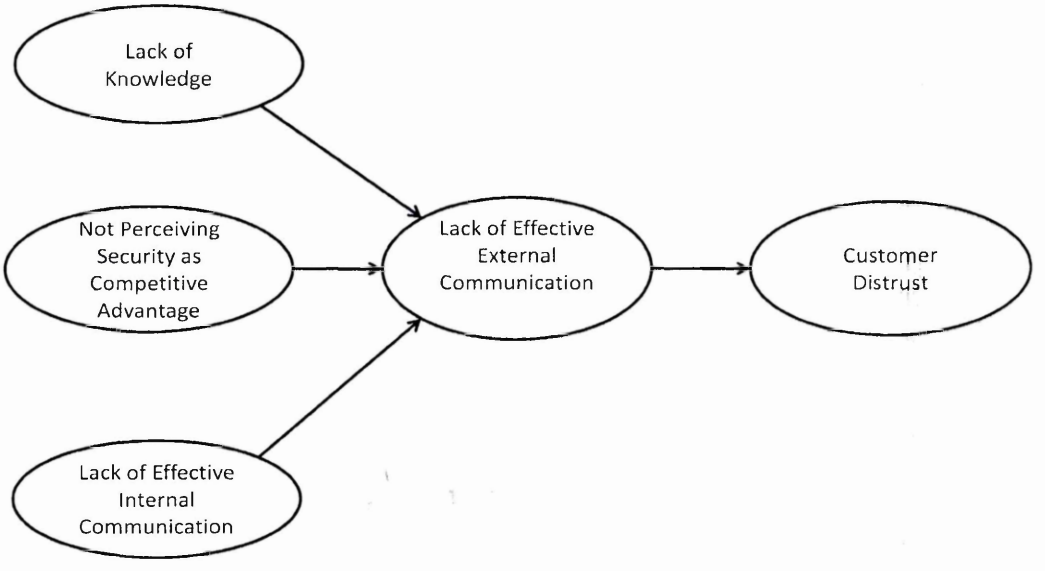

Figure 8.4: Factors affecting external communication and its security implications.

8.1.4 Security policy and its implications for responsibility

From the study it has become apparent that the lack of internal stakeholders' support delayed the implementation of a security policy, which was initially overlooked. The findings also reveal that the idea that security issues can be solved technically by deploying technological solutions was predominant in security stakeholders. This technical orientation of the internal stakeholders combined with the lack of security related knowledge, especially from a strategic point of view, left the company without a security policy which is, as Baskerville & Siponen (2002) pointed out, an essential component for a comprehensive security approach.

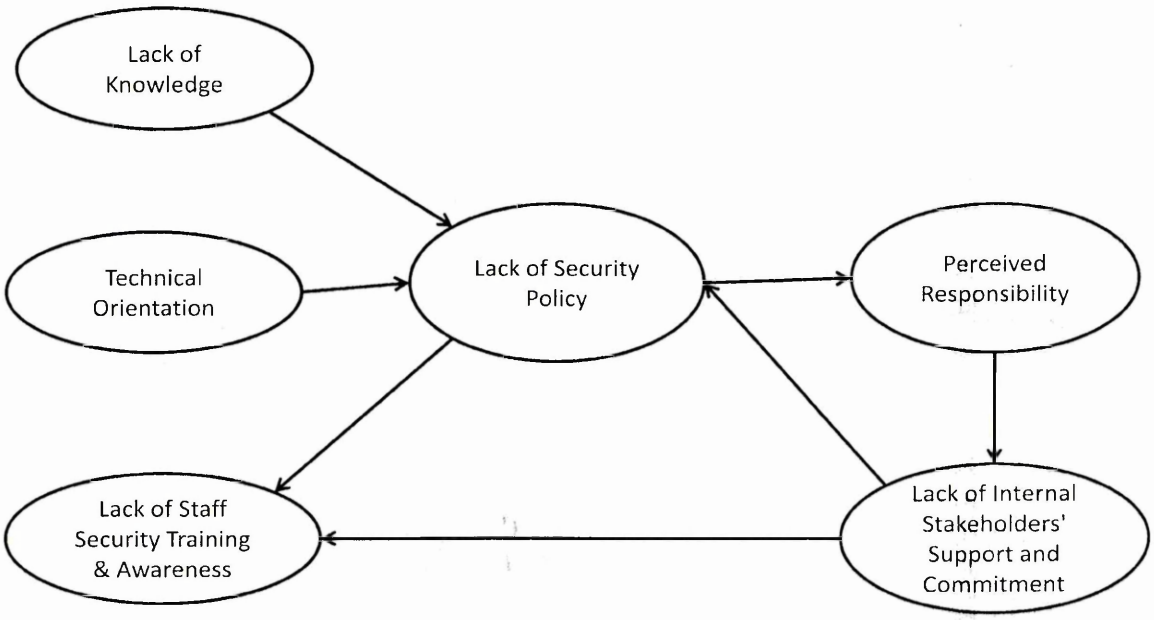

Figure 8.5: Lack of security policy and its implications.

The lack of such a policy led to a situation in which the company staff did not receive any sort of security awareness training to provide them with the necessary skills to ensure secure business environments. Some participants argued that security policy should address the insider risk and that without a security policy it is difficult to get people to be accountable. This illustrates how the lack of a security policy made individuals' responsibility toward security unclear and subject to their personal judgments.

8.1.5 Lack of leadership and decision making power

Adoption of e-Business requires the introduction of many changes in the business environment. However, because of the lack of leadership and decision making power the IT department was unable to introduce those changes until top management became involved and discussed them with the heads of the departments where the changes needed to be applied. As this further supports the previous finding concerning the effect of top management involvement, it also highlights the issue of the inability of the IT people to take and enforce security-related decisions. Such a situation does not encourage introducing security related changes or initiatives such as staff awareness training and security policy. IT lack of leadership and decision making power could impact on the internal stakeholders' willingness to support and commit to security especially when there is conflict between the internal security stakeholders (Wang, 2005). This study showed that the whole focus was on fulfilling requirements specified by business people who appreciate functionality and ease of use more than security. Many participants suggested that empowering IT is one of the things top management should do to improve security. Both the lack of internal stakeholders' support and IT's lack of power did not help eliminating the effects of staff culture and resistance to change, which were highlighted by a number of participants as among the obstacles to providing effective security.

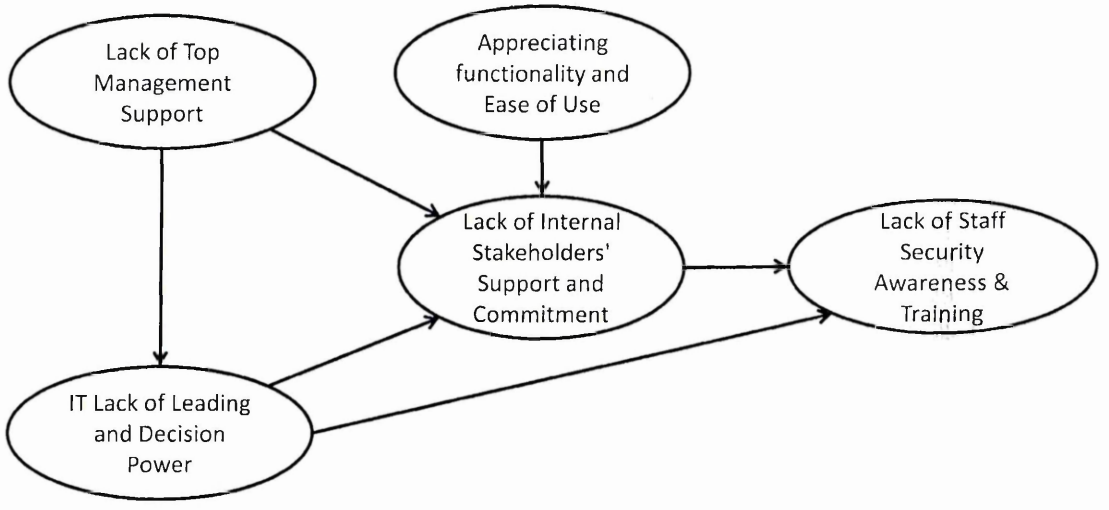

Figure 8.6: The effect of IT lack of power on internal stakeholder support and commitment.

This is supported by Dhillon (2007) who argued that the success of information security initiatives depends on the level of support from different organisational groups, including executive management, IT department, and end users. This has been encapsulated in Figure 8.6.

8.1.6 Staff security awareness and its implications

The study's findings suggest that lack of security training and awareness contributed to create a business environment with a high risk of security breaches which were a result of staff negligence, human error, or malicious behaviour. For instance, in the second unit of analysis, credit card information, which can help in reducing online fraud cases, was not collected because of the inattention of new staff. Other security breaches were related to abuse of the privileges which had been given to employees to carry out specific tasks related to their jobs.

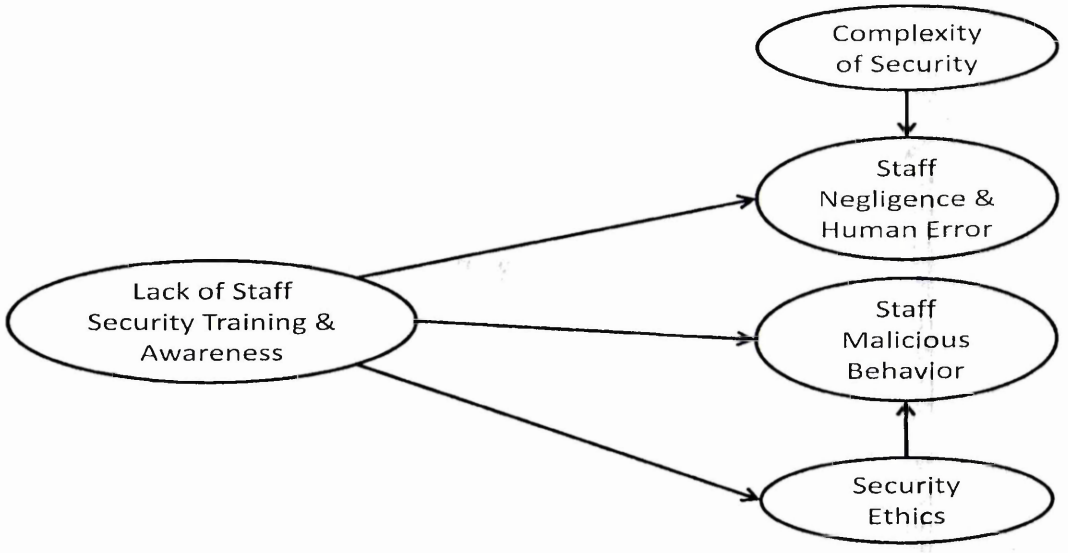

Figure 8.7: Factors affecting staff security behaviour.

Technological complexity and lack of security ethics were other factors that contributed to an increase in human factor risks. The analysis shows that the complexity of some security systems such as the fraud screening system contributed to increasing security breaches by increasing the chance of human error. A similar issue was reported by Werlinger et al. (2009), who found in their study that the difficulty of using some security tools complicated

the task of security practitioners. On the other hand, participants argued that ethics are important to reduce such staff security related issues. Although the effect of company codes of ethics regarding computer abuse could be considered relatively small (Harrington, 1996), the researcher believes that addressing the ethical dimension in designing an information security awareness program should be based on proper motivational and physiological foundations, as is suggested by Siponen, (2000); it can reduce the effect of improper security behaviour by the users.

8.1.7 Security as an add-on component

The study found that the primary driving force for adopting e-Business was to fulfil the technological requirements of some external stakeholders and it was a challenge for the company to meet these requirements, which touch on all the business aspects, in a very short time frame which had been set by the external stakeholders. This forced the company to follow "shortcuts" to save time and to reach the required stage as soon as possible. One of the shortcuts was to treat security as a non-functional requirement which could be added later. The adoption process, which included acquisition of many e-Business applications, was not well planned, especially from a security point of view, and functionality, performance and ease of use were given greater priority. As a result security was overlooked and was not an integral part of the adoption process, which could contribute to possible conflict between system properties (Baskerville, 1992) or between security stakeholders (Lee at al. 2002) when security needs to be added later. The security implications of such an approach have been discussed by many researchers who called for integrating security in every step of an information system development process. For instance Baskerville (1988, 1992) discussed how such a mechanistic approach, which depends on adding security to a complete functional system, can lead to developing security features that may prevent particular proper system functions or prevent the system from adapting to environmental changes. Mouratidis et al. (2004) argued that when security needs to be added into a pre-exiting design this leads to design challenges that most likely cause security holes. In both cases a system needs to be modified either to maintain its functionality or increase its security, which implies an extra cost that the company needs to pay every time such an issue emerges in its e-Business systems.

Another shortcut that the company followed was the outsourcing of some e-Business processes to third party providers. In addition to saving time, there were other factors which encouraged the company to outsource part of its e-Business. First, the lack of e-Business and security related knowledge were clear at the beginning of the adoption process, which made the company depend on the technology providers in two points; software acquisition and outsourcing. Second, the company tried to cut costs and avoid the inconvenience as security was perceived as a costly and complex matter. Unfortunately, the outsourcing process was not based on a well-defined security requirements process to evaluate the security risks associated with the outsourcing process (Earl, M. 1996; Alner, M. 2001). This explains why security was an afterthought in many of its e-Business applications, as in the e-payment application discussed in Chapter 5.

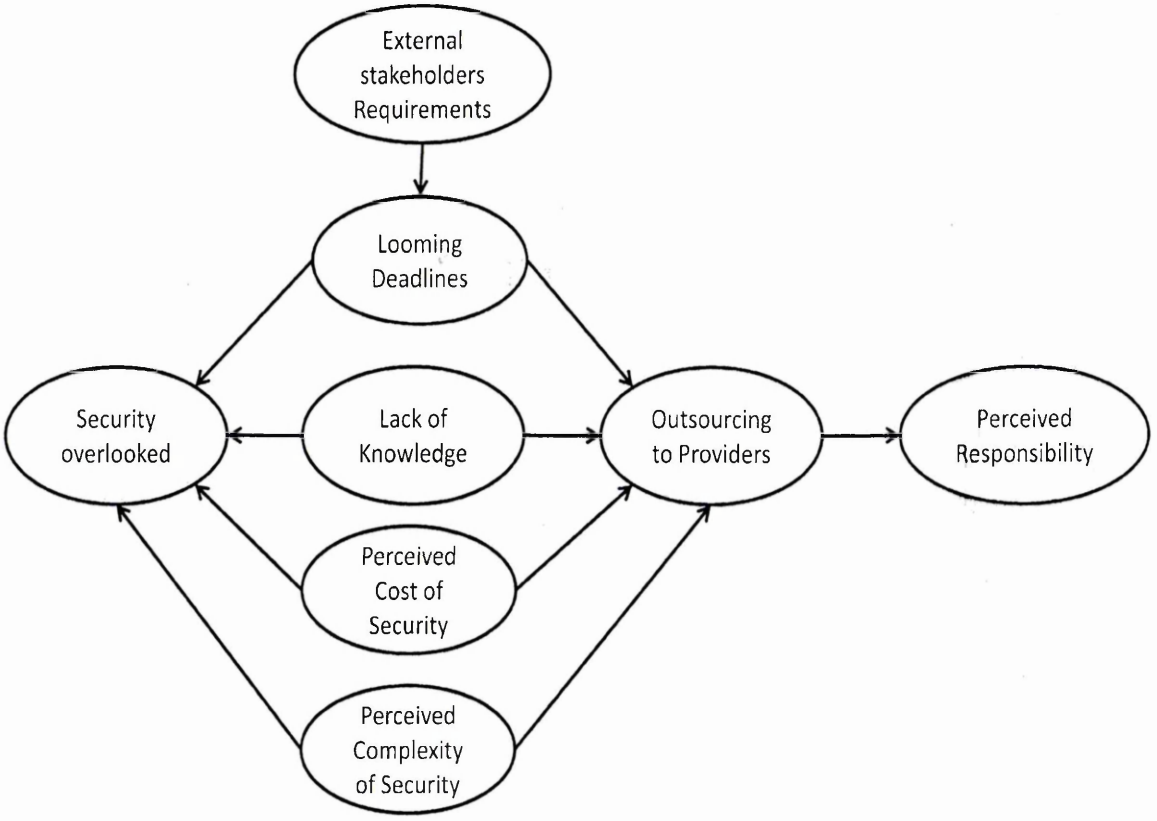

Figure 8.8: Factors making security an add-on component and outsourcing implications.

While few studies explored the socio-technical security effects of outsourcing on internal organisation (see for example Khalafan, 2004), our study found outsourcing had a clear impact on the security perceptions of internal stakeholders. The impact of outsourcing and dependency on third party products on the internal stakeholders' perceptions of security was notable during the field study. Many participants argued that they did not need to worry about e-Business security because it was ensured by the providers who take care of their products' security. Other participants have opted for the assumption that the IT department has nothing to do with e-Business security, as most of the applications were hosted with external third parties. These examples illustrate the effect of outsourcing on the internal stakeholders' perceived responsibility toward e-Business security. Figure 8.8 shows the rich relationship between external stakeholders' requirements, outsourcing and internal stakeholders' perceptions.

8.1.8 Effect of the absence of an effective governmental role

The findings highlighted the absence of an effective governmental role in respect of its responsibility to regulate the digital environment to protect both business and customers; participants argued that the government's role should include other responsibilities such as spreading knowledge, building awareness, and providing guidance about e-Business and security. As the study revealed, the lack of knowledge and guidance affected the way of addressing e-Business security.

Accordingly, the findings suggest that the government could contribute in building security knowledge at both organisational and individual levels. For instance, the study found that the lack of a government monitoring role has two implications. On the business side, nobody checks whether or not private companies are capable from a security point of view of doing business online, and this can impact negatively on the perceived responsibility toward security, especially at the management level inside organisations willing to adopt e-Business. On the other hand, lack of monitoring could increase customers' feelings of distrust in the electronic environment, especially in a context in which there is no legal setup to protect online customers (Privacy International, 2007).

These findings concur with Papazafeiropoulou et al.'s (2001) study which considered the government as an essential stakeholder in the e-Business environment. A recent study

(Knapp et al. 2006) suggested a list of action that the government can do to help towards information security; these include actions such as knowledge dissemination, statutory and legislation action, assigning responsibility, and increasing penalties. This further supports the findings of this study regarding the role of government towards security of the e-business environment. Figure 8.9 shows the previously discussed implications of the current government role in the e-Business environment.

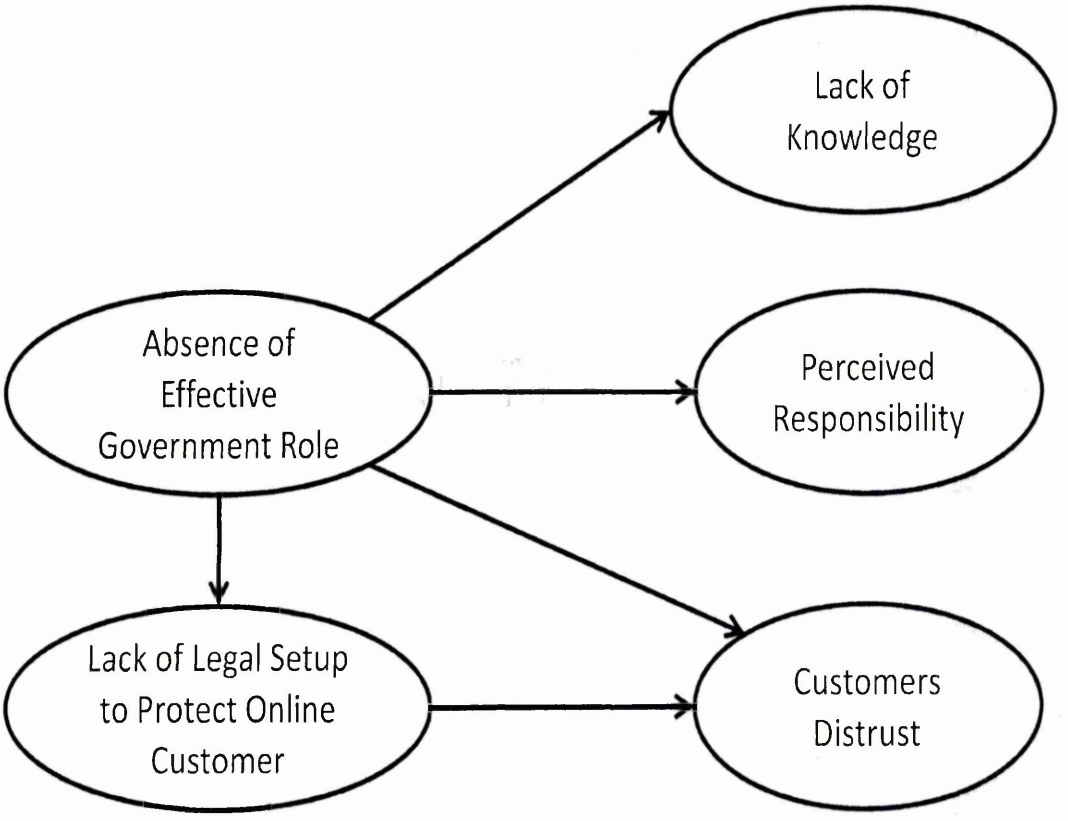

Figure 8.9: The effect of the absence of an effective governmental role on e-Business security.

8.1.9 Factors underlying the customer side of the security problem

Customers represent a human element that interacts with technological elements which have been designed and secured by technologists who usually do not pay much attention to understanding the human element and its social setting (Odlyzko, 2003). To overcome this problem, this study has attempted to understand the customers' security related issues. Based on the study's findings, it can be argued that many customer related aspects need to be considered in order to elevate e-Business security. These security aspects include customers' perceptions and concerns, customers' security knowledge, and interaction with other stakeholders.

As the study showed, security is considered by customers as an important requirement for e-Business. The study found that this appreciation of the value of security is fostered by perceived threats of the electronic environment and the fear of being subjected to these online threats. Furthermore, it revealed that these security concerns are a major factor in customers' reluctance to engage in e-Business transactions. Prior research (Suh & Han, 2003; Flavián & Guinalıú, 2006) acknowledged the strong relation between security and customers' feelings of trust, which in turn reflect on their willingness to engage in real online transactions. Notably, many other factors such reputation, ease of use, and usefulness may affect customer trust and the decision to transact with a particular online merchant or not. Although the study acknowledges the importance of these factors, it strongly suggests that security is considered to be prerequisite that needs to be fulfilled before a customer considers other factors. This confirms other findings which suggest that security has a greater influence on the customer's intention to purchase from e-commerce websites than ease of use or usefulness of purchasing products (Salisbury et al., 2001; Lee, 2002).

In contrast to many previous studies (Alsmadi, 2002; Halaweh & Fidler, 2008; Khasawneh et al., 2009), which just identify customers' security perceptions as a barrier to the adoption of e-Business, this study provides deeper and richer insights into the factors underlying the customer side of e-Business security problem; see Figure 8.10.

This study showed that these perceptions of insecurity were a result of complex and interacting socio-technical factors (interactions with and expectations about other stakeholders as well as awareness and knowledge related factors) which collectively

affected the customers' perceptions of security and how they interacted with the e-Business environment. A discussion of these factors in the light of the relevant literature is given below.

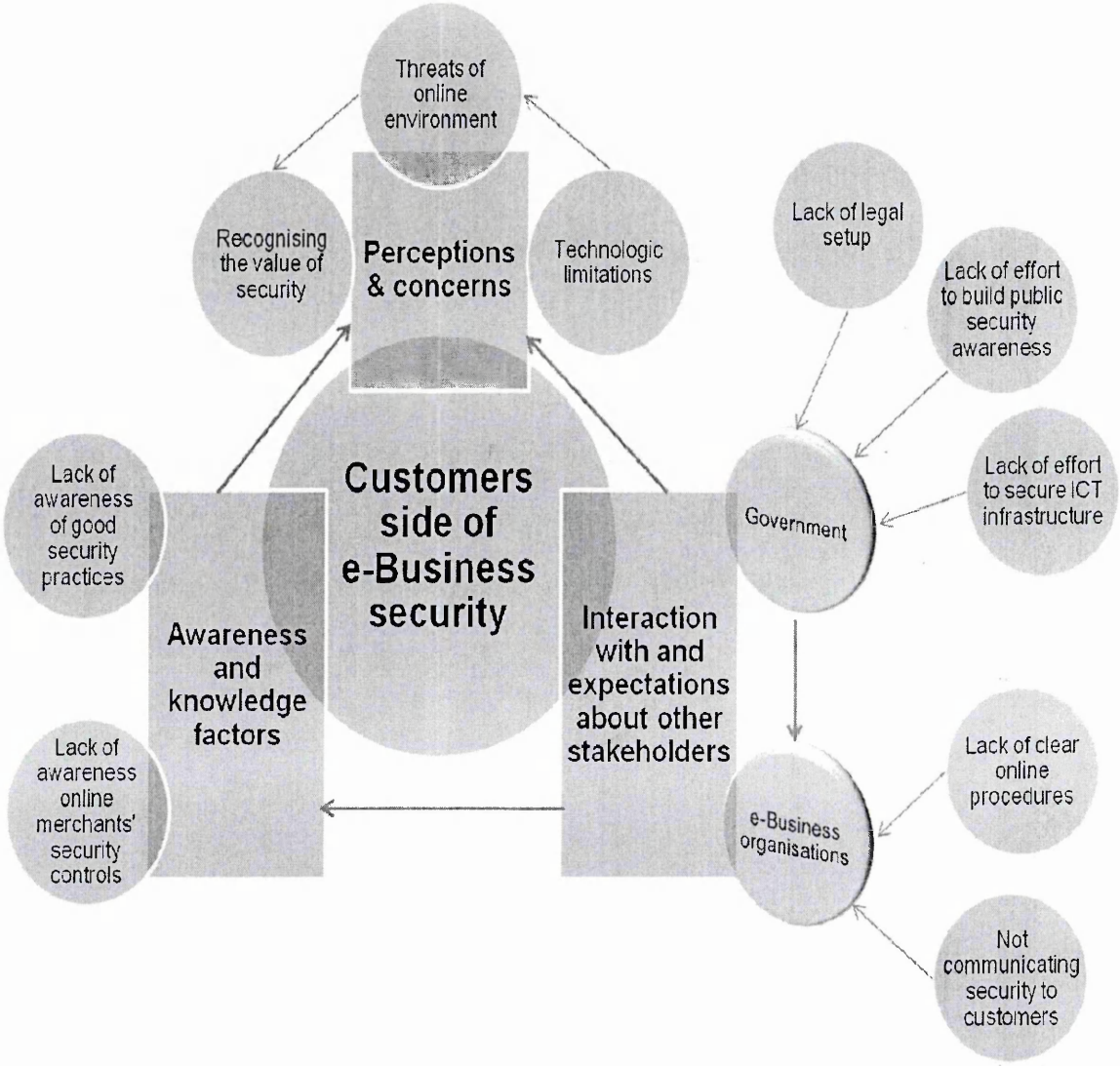

Figure 8.10: Factors underlying the customers' side of e-Business security problem.

At the technical level, the limitations and complexity of human-made technologies as well as the inability of security systems to provide ultimate protection for these technologies are among the factors which contribute to increase customers' e-Business security concerns. All the recent security reports suggest that vulnerabilities in software are increasing dramatically. For instance, SANS @RISK public vulnerabilities database has reported

during 2006-2007 more than 4000 vulnerabilities in Web applications and other commonly used applications such as operating systems, office software and even anti-viruses (SANS, 2009). Several explanations for this continuous growth of software security problems have been provided by the security research community. Security researchers asserted that software developers still lack awareness of secure programming techniques and secure software design principles, therefore, vulnerabilities continue to appear (Ahmad, 2007; Howard, 2008). Other researchers highlighted the negative effect of growing software complexity on security. McGraw (2004) argued that software security represents a critical aspect of the security problem. He continued: "*Internet-enabled software applications present the most common security risk encountered today, with software's ever-expanding complexity and extensibility adding further fuel to the fire*" (p. 2). Schneier (2004) described complexity as "*the worst enemy of security*" because it makes it harder to analysis and test software, which increases the chance that software will contain security flaws. Thus, it seems that all the advances in e-Business applications and their interesting features offered to online customers are a result of increased complexity which in turn affects security. This suggests that customer concerns about the security of internet applications are legitimate and, as customers still suffer from these technical vulnerabilities which create a barrier to the full engagement in e-Business transactions, this increases the burden on technology vendors to develop their security skills and practices in order to reduce security holes in e-Business applications.

While a large number of security threats are a result of technical vulnerabilities, this study found that it is difficult to prevent other security threats technically and customers are required to make good security decisions in order to protect themselves. Replying to fraudulent e-mails and choosing weak passwords are examples of such security threats in which the customer is the central point of protection. In such a situation customers' lack of security knowledge negatively affects their ability to take effective security-related decisions while they interact with an e-Business environment. They make decisions based on a limited amount of information and this could lead to undesired security behaviours which contradict their security perception (Acquisti & Grossklags, 2004) and put their sensitive information at risk. To increase customers' ability to take rational security decisions, they need to be made aware of good security practices. In highlighting the importance of information security awareness outside the organisational dimension,

Siponen (2001) argued that it should be part of the general knowledge of citizens in any information society. This implies introducing the concept into educational systems and public awareness initiatives. As the findings suggest, both public and private sectors could contribute to raising general public awareness of information security aspects. Another aspect of customers' knowledge which needs to be considered is awareness of the mechanisms companies utilise to provide online security. Several security protocols and components, such as digital certificates and secure socket layer (SSL), have been developed to secure online transactions. In addition to the protection that these mechanisms provide, it is assumed that the existence of these security controls on company websites will positively affect customers' security perceptions and elevate their trust levels (Srinivasan, 2004). Unfortunately, when a customer is unaware of such controls it is unlikely that they will affect his/her security perception. In this case, s/he will have a limited amount of information with which to assess the security and trustworthiness of an online merchant, and if s/he decides to make an online transaction with a particular merchant, s/he might depend on other concerns - appearance, brand name, or just word of mouth - which are not necessarily related to the actual security practices of the merchants. These findings concur with Turner's (2003) study which suggested that because customers do not understand technical security controls their perceptions of website security are formed based on factors such as reputation and recommendation. However, Turner's study did not highlight the novelty of this study's findings. These are the need for communicating security to customers and building their awareness of such security controls, which arguably could improve their security assessments in two significant ways. First, customers' concerns might be alleviated when they are made aware of these security controls, and furthermore their existence might increase their perception that a merchant is secure and trustworthy. Second, the researcher argues that this knowledge empowers customers to have real control which can be used alongside their anecdotal recommendations and common sense perceptions to assess online merchant security.

At the organisational level, the findings suggest that e-Business organisations need to show more commitment to security in order to overcome the customers' security concerns. Online companies should realise that these security concerns are legitimate and based on real security threats associated with e-Business activities. These companies should understand, evaluate and systemically address these risks. They need to know that the

internet, which is the medium for conducting their businesses, is inherently insecure (Ghosh, 1998) and any computer or application which is connected to this medium is likely to be attacked more than at any time before. As security attacks shift from simple and generic attacks to more sophisticated and targeted ones, e-Business organisations need to adopt more powerful security controls, including strong authentication, online and offline encryption, and fraudulent transaction detection systems (Slewe & Hoogenboom, 2004). Of equal importance, the internal threats to e-Business organisations need to be considered (McCrohan, 2003). Customers' information can be subject to risks which come not from the internet but from inside an online company itself. Security uneducated staff, disgruntled employees, omission, negligence, and the lack of understanding of the value of security by top management, are all examples of such internal security threats that need to be addressed. Yet technical security solutions alone are not enough to provide adequate protection or the level of confidence that customers want in e-Business transactions. Dealing with inside threats requires a set of technical, organisational, procedural and physical security controls, which are based in a well-established information security risk management plan. Moreover, the study suggests that, in addition to deploying web security controls and addressing the internal risk, security needs to be promoted and communicated to customers. If customers are not effectively informed about the company's actual practices to protect information, the existence of the above security measures, which provide a practical and real security, might not be sufficient to reduce the customer's security fears. This is because security is both perception and reality, and these are not the same (Schneier, 2008). This is confirmed by Miyazaki & Fernandez (2000), who found a positive relationship between disclosure of online merchants' security practices and customer perception of online risk and purchasing intentions. Miyazaki & Fernandez contended that if customer privacy and security concerns raise risk perceptions and lower purchasing levels, higher privacy and security disclosure would lessen such concerns, which in turn would reduce perception of risk and increase purchasing levels. While communicating security to customers could improve credibility and transparency, which are considered by customers as important factors in increasing trustworthiness in e-Business, it can be useful in building customers' security knowledge and raising their awareness of different measures that can contribute to increase their online security.

At the legal level, it seems that these security concerns persist partially due the fact that the legal framework and government efforts to ensure security of the digital environment do not meet the customers' expectations. In fact, the political and legal climate in the country can significantly affect e-Business in general (Aljifri et al., 2003) and its security in particular. Prior studies acknowledged the impact of government readiness and involvement on the diffusion of e-Business and other ICT-based applications. Molla and Licker (2005) argued that government has an important role in encouraging the private sector in the country to adopt e-Business by providing supportive infrastructure, legal and regulatory frameworks, policies, and strategies. However, government support varies from country to country and it is below the threshold in many developing countries (UN-ESCWA, 2007). While many previous studies highlighted the role of governments and policy makers in the diffusion of e-Business, this study extended the role of government in the adoption of e-Business to include security related actions. It suggests that the government represents an important security stakeholder with a number of responsibilities that need to be fulfilled in order to ensure security and protect online customer rights. Its responsibility starts with regulating e-Business in the country and enacting the laws that protect customer's privacy and security. It can force online merchants to follow best practice in security and to communicate security to their customers to provide them with some level of assurance. For instance, in many developed countries laws have been issued to force online retailers to disclose their privacy and security practices to the customers in order to increase transparency and trust levels (Miyazaki & Fernandez, 2000). The findings also suggest that government needs to increase penalties for any illegal online activities, such as fraud and credit card abuse, which can deter such actions and reduce risk perceptions. In addition to the legal role in the security of e-Business, customers expect government to have a stake in building general public knowledge of security related aspects. Through national awareness initiatives and giving more attention to the subject in the country's educational system, citizens can be equipped with security knowledge and good skills to use e-Business in a secure way. Consequently, such actions can help in diminishing customers' security concerns and increasing their awareness of both their rights and responsibilities toward security in an e-Business environment.

8.2 Thesis Contribution

This thesis contributes by a framework of inquiry for better understanding of the various issues surrounding security within an e-Business environment. It has defined an interpretive stakeholder approach which has been used to explore all the interested stakeholders and investigate their interrelationships and influences. This contributes to the socio-technical body of research in Information System Security in general and e-Business Security in particular with stakeholder analysis grounded in an interpretive paradigm. Moreover, its findings contribute to a better understanding of e-Business security in the context of Jordan with potential practical implications which span a wide range of stakeholders. This section discusses this thesis's theoretical, methodological and practical contributions.

The theoretical contribution of this thesis stems from the limitations identified in the predominant technical security approaches which consider neither the multifaceted nature of e-Business security nor the requirements and influences of the various stakeholders involved. This study contributed to overcoming this problem by devising a stakeholder analysis combined with a well-designed knowledge-generating approach which gave the possibility of understanding the influence of the social and organisational aspects where technical systems operate. This led to developing a holistic understanding of e-Business security where "e-Business stakeholder" was used as a meta-theory to facilitate deeper understanding of security in an e-Business environment. This was incorporated in a conceptual framework of enquiry which guided the study in exploring the different dimensions influencing e-Business security. Consequently, four major stakeholders in the problem situation were explored and their security implications were identified. These stakeholders included: technology providers, e-Business organisations, government and customers. Through this inductive stakeholder analysis an explanatory framework of organisational, legal, human and technical factors affecting security in e-Business environments was developed. Additionally, the research brought these factors together, identified their interrelationships and implications, and positioned them in the current domain knowledge.

Methodologically, the thesis responded to the predominant positivist approaches to information security and contributed by defining a qualitative interpretive methodology which allowed the research to capture the complexity of e-Business security environment.

The suitability and the need for a more inductive interpretive approach and qualitative research method to look at the security of e-Business were evaluated and justified. This study also contributed by developing a complete research design which showed how a case study method as a research strategy can be combined with a general inductive approach realised through thematic framework analysis to provide a systematic and rigorous methodology.

The practical contribution of the study stems from the rich insight it provides into the problem situation. While previous studies draw our attention to e-Business security in the context of Jordan, they do not offer a deep analysis of the problem situation; this in turn limits our understanding of the various aspects that need to be considered to develop a secure e-Business environment. The limitations emerge from the fact that most of these studies did not consider security as their primary focus; therefore, little effort had been devoted to exploring this issue in detail. Moreover, the positivist approach underlying most of these studies limited their findings into a set of specific questions which often tried to explore the existence of predefined security issues or not without offering an explanation of how and why these issues emerged. In contrast, this study captured the complexity of the problem domain and developed knowledge and understanding of the various associated issues that need to be considered by the identified stakeholders in order to incorporate security in way that provides a trustworthy e-Business environment. The study provided rich insights into the security of e-Business by identifying and interpreting the roles, the perceptions, and the interactions of several groups of security stakeholders. Moreover, it identified several organisational aspects and explained their relationships with security. These aspects, which include issues such as governance, communication, power conflict, awareness, and resistance to change, have potential practical implications at individual, organisational, and national levels. Additionally, the findings provide insights into the customers' side of the security problem and explain its relationships with other stakeholders, including government, business, and technology providers. This is a sound practical contribution as it can help these stakeholders in designing better security approaches based on a deeper understanding of customers' security requirements.

8.3 Interpretive Research Evaluation

All research, whether qualitative or quantitative, must respond to acceptable standards of quality and goodness; these are criteria against which the trustworthiness of the research process and its findings can be evaluated (Marshall & Rossman, 1999). While Positivist researchers depend on the concepts of reliability, validity, and generalisability to evaluate their quantitative studies, it seems that interpretive researchers should not depend on these measures, which are intended to ensure an objectivity and universal applicability that do not fit the nature of qualitative research, which is characterised by its justifiable subjectivity (Auerbach & Silverstein, 2003). Therefore, other evaluation criteria and guidelines have emerged to assess the soundness and the rigour of interpretive studies. Lincoln and Guba's (1985) proposed constructs of credibility, transferability, dependability and confirmability are the most cited principles for establishing trustworthiness in qualitative research (Ryan et al., 2007; Thomas, 2006; Marshall & Rossman, 1999; Miles & Huberman, 1994). This section will discuss these principles in relation to the study's processes and findings in an attempt to assess its quality.

Credibility is concerned with truthfulness of the findings and the extent to which these findings reflect the actual problem situation. Lincoln and Guba (1985) asserted that credibility may be enhanced by several techniques such as prolonged engagement, persistent observation, triangulation, and peer debriefing. Within this study these techniques were used to increase the chance that credible findings and interpretations would be produced. To achieve the prolonged engagement, which required spending sufficient time in the field to understand the context and to build trust with the study's participants, the researcher conducted a field study over a period of 6 months (April-September 2008); prior to that, potential participants, especially site managers, had been contacted and given an overview of the project in order to get their approval and support for the study. This has been discussed in more detail in section 3.6.1. Furthermore, the prolonged engagement was also enhanced by the fact that the researcher is from the same context and has spent most his life there. Credibility was also improved by the use of persistent observation, which aimed to identify "those characteristics and elements in the situation that are most relevant to the problem or issue being pursued and focusing on them in detail" (p. 304), which was achieved by employing the general inductive coding process guided by the study's aims

and objectives. This was discussed in section 3.6.3. Triangulation of data sources was another technique used to increase credibility; while semi-structured interview was the primary data collection technique, it was triangulated with multiple sources of evidence, including document review, and physical artifact review, which were used as corroboratory techniques along with primary data collection techniques. These were discussed in section 3.6.2. Moreover, debriefing was used as an additional technique to establish credibility in this study. This has been achieved through periodic debriefing sessions with the researcher's supervisor and other academic staff who have a great deal of knowledge about the inquiry area and methodological issues. These sessions provided an external evaluation for the research process and ensured clarity of the interpretations.

Transferability is concerned with the possibility of applying the findings of a qualitative study in a context other than the one in question. Transferability depends on the degree of similarity between the sending and receiving contexts (Lincoln & Guba, 1985). A study can be considered transferable when its findings fit other contexts and readers can apply them to their own experiences (Ryan et al., 2007). This implies that the burden of proof that findings are transferable lies on the reader interested in applying them in other contexts; the task of the original researcher "ends in providing sufficient descriptive data to make such similarity judgements possible" (Lincoln & Guba, 1985, p. 298). Therefore, a thick description is usually used as a technique to enhance transferability. In this study, detailed descriptive accounts of the research setting, procedures and findings have been provided to enable other researchers and interested readers to apply the findings or conduct similar studies in their chosen contexts. A thick description, which facilities transferability, is clamed in this study for the following reasons. First, the problem situation was described in the first chapter together with a critical evaluation of previous studies covering the same context. Second, a complete research design, including research strategy, data collection techniques, and analysis procedure, was presented in Chapter 3 with a discussion of the philosophical assumptions which led to this particular research design. This also included a description of the four units of analysis and the purposive sampling techniques followed to choose the study's participants. Third, the emerged themes and their interrelationships were described, grounded in the data, and discussed in relation to the existing body of research.

Dependability is concerned with the transparency of the research process and the possibility of following the steps by which the researcher produced his interpretations (Auerbach & Silverstein, 2003). A study can be considered dependable/auditable if it produces sufficient information and traceable evidence of a decision tail at each stage of the research process (Ryan et al., 2007; Lincoln & Guba, 1985). To meet this criterion, the study used thematic framework analysis, as this facilitates a rigorous, transparent, and systemic way for concocting a qualitative study. This method, which follows the guidelines of the general inductive approach, was described in section 3.6.3 and applied in detail in Chapter 4. The thematic framework was used to classify and organise data according to themes, concepts and emerging categories, which were then linked back to the evidence collected from the field study. This provides the reader with the possibility of following the researcher's steps and potentially arriving at similar or comparable interpretations.

Confirmability is concerned with ascertaining that the findings are derived from the data collected from the field study. The criterion of confirmability requires the researcher to show how interpretations have been reached (Ryan et al., 2007). Lincoln & Guba (1985) suggested that this can easily be verified if appropriate audit trail linkages have been established. Within this study, the use of the thematic framework analysis was an excellent choice for establishing conformability. While it provides a systematic and transparent method for managing and analysing qualitative data, it also provides linkages between the raw data and themes representing the study's findings. The data management phase, described in Chapter 3, represents an essential step for producing the audit trail required to ensure that the study findings are grounded on the data and thereby meet the conformability criterion.

8.4 Limitations

The researcher has adopted an interpretive qualitative approach in which data collection and data analysis phases depend on what is called theoretical sampling; this implies an iterative collection and analysis of data until the theoretical saturation phase is reached.

Despite the fact that the researcher was aware of the nature of qualitative methods which inevitably makes it difficult to estimate reaching the saturation phase accurately, further unanticipated factors contributed to increasing the effort and time required: firstly, the

researcher's lack of familiarity with qualitative analysis techniques involved additional training; secondly, the large volume of data that was collected; and finally, the scarceness of similar studies in the application domain chosen.

Accessibility was another issue experienced in the fourth unit of analysis in which government officials were reluctant to fully engage in face-to-face interviews and tended to give very short responses. This forced the research to depend on document review to explore the current role of the government in the security of e-Business. However, the empirical findings of this unit of analysis were verified against the data collected from the other stakeholders to ensure the credibility of the interpretations.

8.5 Future Directions

While this research contributed by developing a conceptual framework for better understanding security in e-Business environment, further research could investigate how its findings could be used to develop an e-Business security readiness tool to assess whether a country or an organisation is ready from a security point of view to participate effectively in the digital economy. The socio-technical security related factors which emerged from this study could form a foundation for such an instrument and determine the main area on which it should focus.

Another future research could employ an interpretive stakeholder analysis to explore security aspects of other emerging fields such e-Government (HjoujBtoush et al., 2009) and e-Learning (Qteishat, 2010). These fields are starting to attract more attention, especially in developing countries which are trying to get the most from ICT diffusion. Therefore, stakeholder analysis could be a powerful tool to uncover their interrelated security issues.

From methodological point of view, the interpretive approach to e-Business security adopted in this research gave the possibility of understanding the influence of the social and organisational aspects of the context in which e-Business systems operate. On the other hand, a possible future direction based on a "Critical thinking" can go beyond this interpretive understanding to achieve emancipatory social change (Walsham, 1993, Brook, 2002). This is because a lack of security can be viewed as a source of alienation which restricts people, organisations and even countries from benefiting from the prosperity e-Business might bring to them. We argued in (Siddiqi et al., 2010) that a lack of security can

negatively affect national initiatives and strategies that are attempting to bridge the digital gap. Consequently, this absence of security would increase the chance that a country stays longer on the wrong side of the global digital divide and people in this country are being excluded from receiving the claimed advantages of the electronic evolution. It is argued that "Any approach that claims an emancipatory intent should be able to promote participation and take account of unequal power relations" (Brooke, 2002, p. 50). Therefore, a critical approach to e-Business security would help in revealing emerging contradictions, related conflicts and empowering people in a way that would increase the chance of having security e-Business environment which considers the needs and influences of all the relevant stakeholders.

Additional future work could employ an "Action Research" to see how the knowledge gained from this empirical work can be used again to introduce changes that would influence the current state of e-Business security in the problem situation. Action research is described as a method that "combines theory and practice (and researchers and practitioners) through a change and reflection on an immediate problematic situation... Action research is an iterative process involving researchers and practitioners acting together on a particular cycle of activities, including problem diagnosis, action intervention, and reflective learning." (Avison et al., 1999, p. 94). It is an interventionist method; this implies that the researcher needs be an active participant in the problem domain. Baskerville and Wood-Harper (1996) described Lewin's (1951) original model of action research; this model included iteration of six stages: 1- Analysis, 2- Fact-finding, 3- Conceptualising, 4- Planning, 5- Implementation of Action and 6- Evaluation. Considering the conceptual framework developed by this study it can be argued that the first three stages of action research have been covered in here and if there is a future opportunity for the researcher (or other interested researchers) to be an active participants in the same problem domain the full action research cycle can be complete.

References

ABAWAJY, J., THATCHER, K. and KIM, T. (2008). Investigation of stakeholders commitment to information security awareness programs. In: *International Conference on Information Security and Assurance, ISA 2008.* 472-476.

ACQUISTI, A. and GROSSKLAGS, J. (2004). Privacy attitudes and privacy behavior: Losses, gains, and hyperbolic discounting. *The economics of information security.kluwer academic publishers,* .

AHMAD, D. (2007). The contemporary software security landscape. *IEEE security & privacy,* **5** (3), 75-77.

AL NAGI, E. and HAMDAN, M. (2009). Computerization and e-government implementation in Jordan: Challenges, obstacles and successes. *Government information quarterly,* **26** (4), 577-583.

AL-IBRAHEEM, M. and TAHAT, H. (2006). Regulating electronic contracting in Jordan. [online]. In: *21st BILETA Conference: Globalisation and Harmonisation in Technology Law,* 2006.

AL-JAGHOUB, S. and WESTRUP, C. (2003). Jordan and ICT-led development: Towards a competition state? *Information technology & people,* **16** (1), 93-110.

ALJIFRI, H. A., PONS, A. and COLLINS, D. (2003). Global e-commerce: A framework for understanding and overcoming the trust barrier. *Information management and computer security,* **11** (2/3), 130-138.

ALNER, M. (2001). The effects of outsourcing on information security. *Information systems security,* **10** (2), 1-9.

AL-QIRIM, N. (2004). A framework for electronic commerce research in small to medium-sized enterprises. *Electronic commerce in small to medium-sized enterprises: Frameworks, issues and implications.,* .

AL-QIRIM, N. (2007). The adoption and diffusion of e-commerce in developing countries: The case of an NGO in Jordan. *Information technology for development,* **13** (2), 107-131.

ALSMADI, S. (2002). Consumer attitudes towards online shopping in Jordan: Opportunities and challenges. In: *the First Forum for Marketing in Arab Countries,* 2002.

AMEinfo (2007). *Royal Jordanian rated as advanced in e-commerce by IATA.* [online]. Last accessed 15/03 2009 at: http://www.ameinfo.com/134346.html.

AMOR, D. (2000). *The e-business revolution: Living and working in an interconnected world.* Prentice Hall, NJ.

ANDERSEN, C. (2004). Visa Jordan selects STS' PayONE solution. *AMEinfo,* .

ANDERSON, J. (2003). Why we need a new definition of information security. *Computers & security,* **22** (4), 308-313.

ARTHUR, S. and NAZROO, J. (2003). Designing fieldwork strategies and materials. In: RITCHIE, J. and LEWIS, J. (eds.). *Qualitative research practice.* London, SAGE, .

AUERBACH, C. F. and SILVERSTEIN, L. B. (2003). *Qualitative data: An introduction to coding and analysis.* NYU press.

AVISON, D., et al. (1999). Action research. *Communications of the ACM,* **42** (1), 97.

AVISON, D. and WOOD-HARPER, T. (1990). Multiview methodology. *Blackwell scientific publishers, Oxford.,* .

BACKHOUSE, J. and DHILLON, G. (1996). Structures of responsibility and security of information systems. *European journal of information systems,* **5** , 2-9.

BAKARI, Jabiri (2007). *Holistic approach for managing ICT security in non-commercial organisations. A case study in a developing country.* [online]. PhD.

BALLMER, S. (2004). *Net security is everyone's problem not just Microsoft's.* [online]. Last accessed 03/10 2009 at: www.techworld.com.

BAROAUSKAS, P. and SARAPOVAS, T. (2004). PROBLEMS OF E-BUSINESS IMPLEMENTATION IN SMEs.

BASKERVILLE, R. (1988). *Designing information systems security.* Chichester, J. Wiley.

BASKERVILLE, R. (1992). The developmental duality of information systems security. *Journal of management systems,* **4** (1), 1-12.

BASKERVILLE, R. and SIPONEN, M. (2002). An information security meta-policy for emergent organizations. *Logistics information management,* **15** (5/6), 337-346.

BASKERVILLE, R. and WOOD-HARPER, T. (1996). A critical perspective on action research as a method for information systems research. *Journal of information technology,* **11** (3), 235-246.

BENBASAT, I., GOLDSTEIN, D. and MEAD, M. (1987). The case research strategy in studies of information systems. *MIS quarterly,* , 369-386.

BEZNOSOV, K. and BEZNOSOVA, O. (2007). On the imbalance of the security problem space and its expected consequences. *Information management & computer security,* **15** (5), 420-431.

BISHOP, M. (2003). *Computer security: Art and science.* Addison-Wesley.

BISHOP, M. (2004). *Introduction to computer security.* Addison-Wesley.

BOLAN, C. and MENDE, D. Computer security research: Approaches and assumptions. In: *2nd Australian Information Security Management Conference,* 115.

BRAUN, V. and CLARKE, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology,* **3** (2), 77-101.

BROOKE, C. (2002). What does it mean to be 'critical' in IS research? *Journal of information technology,* **17** (2), 49-57.

BRYMAN, A. (2001). *Social research methods.* 3rd ed., UK, Oxford.

BURGOYNE, J. (1994). Stakeholder analysis. In: CASSEL, C. and SYMON, C. (eds.). *Qualitative methods in organizational research: A practical guide.* London, SAGE, 187-207.

CASSELL, C. and SYMON, G. (2004). *Essential guide to qualitative methods in organizational research.* London, SAGE.

CHAPMAN, P., et al. (2000). Building internet capabilities in SMEs. *Logistics information management,* **13** (6), 353-360.

CHECKLAND, P. (1981). *Systems thinking, systems practice.* Chichester, J. Wiley.

CHEN, M. (2003). Factors affecting the adoption and diffusion of XML and web services standards for E-business systems. *International journal of human-computer studies,* **58** (3), 259-279.

CHOI, N., et al. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information management & computer security,* **16** .

CHUA, C., et al. (2005). The evolution of e-commerce research: A stakeholder perspective. *Journal of electronic commerce research,* **6** (4), 262-281.

CHUA, W. (1986). Radical developments in accounting thought. *The accounting review,* **61** (4), 601-632.

CLARKE, Roger (2000). *Electronic commerce definitions* [online]. 2009 at: http://www.rogerclarke.com/EC/ECDefns.html.

CRESWELL, J. (2002). *Educational research: Planning, conducting, and evaluating quantitative and qualitative approaches to research.* Upper Saddle River, NJ, Pearson Education.

CRESWELL, J. (2007). *Qualitative inquiry & research design; choosing among five approaches.* 2nd ed., SAGE-UK.

CUNNINGHAM, P. and FROSCHL, F. (1999). *Electronic business revolution.* Springer.

DADA, D. (2006). eReadiness for developing countries: Moving the focus from the environment to the users. *EJISDC,* **27** (6), 1-14.

DANIEL, E., WILSON, H. and MYERS, A. (2002). Adoption of e-commerce by SMEs in the UK. *International small business journal,* **20** (3), 253-270.

DAVIDSON, M. (2008). Who pushed vendors toward better security? *CSO,* .

DE GRAAF, X. and MUURLING, R. (2003). Underpinning the eBusiness framework-defining eBusiness concepts and classifying eBusiness indicators. In: *16th Bled eCommerce Conference: ETransformation, R. Wigand, Y. Tan, J. Gricar, A. Pucihar & T. Lunar (Editors.), University of Maribor, Slovenia, Bled, Slovenia,* .

DEŽELAK, Z., STERNAD, S. and BOBEK, S. (2006). Comparative analysis of E-business implementation critical success factors. *Organizacija,* **39** .

DHILLON, G. (1995). *Interpreting the management of information systems security.* PhD. London School of Economics and Political Sciences.

DHILLON, G. and BACKHOUSE, J. (2000). Technical opinion: Information system security management in the new millennium.

DHILLON, G. and BACKHOUSE, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information systems journal,* **11** (2), 127-153.

DONALDSON, T. and PRESTON, L. (1995). The stakeholder theory of the corporation: Concepts, evidence, and implications. *The academy of management review,* **20** (1), 65-91.

EARL, M. (2000). Evolving the e-business. *Business strategy review,* **11** (2), 33-38.

EARL, M. J. (1996). The risks of outsourcing IT. *Sloan management review,* **37** , 26-32.

EISENHARDT, K. (1989). Building theories from case study research. *Academy of management review,* , 532-550.

ESCWA (2005). *The national profile for information society in Jordan.* [online]. Last accessed 12/30 2009 at: http://www.escwa.un.org/wsis/reports/docs/Jordan_2005-E.pdf.

ESCWA (2007). *Regional profile of the information society in western Asia.* [online]. United Nation. (E/ESCWA/ICTD/2007/15) at: http://www.escwa.un.org/information/pubdetails.asp.

ESCWA (2009). *Building trust in E-services in the ESCWA region.* [online]. United Nations. (E/ESCWA/ICTD/2009/4) at: http://www.escwa.un.org/information/publications/edit/upload/ictd-09-4-a.pdf.

ETL (2001). *Electronic transactions law no. 80 of 2001*Jordan, .

FLAK, L. and ROSE, J. (2005). Stakeholder governance: Adapting stakeholder theory to e-government. *Communications of the association for information systems,* **16** (1), 31.

FLAVIÁN, C. and GUINALIÚ, M. (2006). Consumer trust, perceived security and privacy policy. *Industrial management and data systems,* **106** (5), 601-620.

FLECHAIS, I. and SASSE, M. A. (2009). Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-science. *International journal of human-computer studies,* **67** (4), 281-296.

FOSSEY, E., et al. (2002). Understanding and evaluating qualitative research. *Australasian psychiatry,* **36** (6), 717-732.

FREEMAN, R. (1984). *Strategic management: A stakeholder perspective.* Cambridge, Ballinger.

FRYNAS, J. (2002). The limits of globalization- legal and political issues in e-commerce. *Management decision,* **40** (9), 871-880.

FURNELL, S. M. and KARWENI, T. (1999). Security implications of electronic commerce: A survey of consumers and businesses. *Internet research: Electronic networking applications and policy,* **9** (5), 372-382.

GEER, D. (2004). Just how secure are security products? *Computer,* , 14-16.

GHOSH, A. K. (1998). *E-commerce security: Weak links, best defenses.* Wiley.

GOLDEN, L. (2006). STS launches Jordanian housing bank portal. *AMEinfo,* .

GREGORIO, D., KASSICIEH, S. and NETO, R. (2005). Drivers of e-business activity in developed and emerging markets. *IEEE transactions on engineering management,* **52** (2), 155-166.

GROUCUTT, J. and GRISERI, P. (2004). *Mastering e-business.* Palgrave Macmillan.

GUEST, G., BUNCE, A. and JOHNSON, L. (2006). How many interviews are enough?: An experiment with data saturation and variability. *Field methods,* **18** (1), 59.

HALAWEH, M. and FIDLER, C. (2008). Security perception in E-commerce: Conflict between customer and organizational perspectives. *Computer science and information technology, 2008.IMCSIT 2008. International multiconference on computer science and information technology.* , 443-449.

HARRINGTON, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS quarterly,* , 257-278.

HARTLEY, J. (2004). Case study research. In: CASSELL, C. and SYMON, G. (eds.). *Essential guide to qualitative methods in organisational research.* London, SAGE, 323-333.

HJOUJ BTOUSH, M. (2009). *Evaluation of E-goverment services in jordan: Providers' & users' perception.* PhD. Sheffield Hallam University.

ICT-POLICY (2007). *Statement of government policy on information and communication technology and postal sectorsJordan*, at: http://www.moict.gov.jo/Gov%20POLICY%20%202007%20ICT%20and%20Postal%20Sectors%20Eng%20an.pdf.

IIVARI, J. and HIRSCHHEIM, R. (1996). Analyzing information systems development: A comparison and analysis of eight IS development approaches. *Information systems,* **21** (7), 551-575.

IT Governance Institute (ed.) (2006). *Information security governance: Guidance for boards of directors and executive management.* 2nd ed., USA, .

JAMES, H. (1996). Managing information systems security: A soft approach. In: *Proceedings of the Information Systems Conference of New Zealand,* 10-20.

JENNEX, M. and AMOROSO, D. (2002). e-business and technology issues for developing economies: A Ukraine case study. *The electronic journal of information systems in developing countries,* **10** (0).

JIWNANI, K. and ZELKOWITZ, M. (2002). Maintaining software with a security perspective. In: *Proceedings of the International Conference on Software Maintenance,* 194-203.

JONES, S., MORRIS, M. and MASERA, M. (2000). Trust requirements in E-business: A conceptual framework for understanding the needs and concepts of different stakeholders. *Communications of the ACM,* **43** (12).

JOSSELSON, R. and LIEBLICH, A. (2003). A framework for narrative research proposals in psychology. *Up close and personal: The teaching and learning of narrative research,* , 259-274.

KAJAVA, J., et al. (2006). Information security standards and global business. *Industrial technology,* , 15-17.

KALAKOTA, R. and ROBINSON, M. (2001). *E-business 2.0: Roadmap for success.* Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA.

KAPLAN, B. and MAXWELL, J. (1994). Qualitative research methods for evaluating computer information systems. *Evaluating health care information systems: Methods and applications,* , 45-68.

KATSIKAS, S., LOPEZ, J. and PERNUL, G. (2005). Trust, privacy and security in e-business: Requirements and solutions. *Lecture notes in computer science,* **3746** , 548.

KHALFAN, A. M. (2004). Information security considerations in IS/IT outsourcing projects: A descriptive case study of two sectors. *International journal of information management,* **24** (1), 29-42.

KHASAWNEH, A., AL AZZAM, I. and BSOUL, M. (2009). A study on e-commerce security in Jordan. *International journal of electronic finance,* **3** (2), 166-176.

KIM, C., et al. (2009). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic commerce research and applications,* .

KING, N. (2004). Using interviews in qualitative research. In: CASSELL, C. and SYMON, G. (eds.). *Essential guide to qualitative methods in organizational research.* London, SAGE, .

KIOUNTOUZIS, E. (2004). Approaches to the security of information systems. In: KATSIKAS, S., GRITZALIS, D. and GRITZALIS, S. (eds.). *Information systems security.* Athens, Greece, New Technologies, .

KLEIN, H. and MYERS, M. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS quarterly,* **23** (1), 67-93.

KNAPP, K., et al. (2006). The top information security issues facing organisations: What can government do to help? *EDPACS,* **34** (4), 1-10.

KNORR, K. and RÖHRIG, S. (2001). Security requirements of e-business processes. *Towards the E-society: E-commerce, E-business, and E-government,* , 73.

KOWALSKI, S. (1994). *IT insecurity: A multi-disciplinary inquiry.* PhD. Department of Computer and System Sciences (Royal Institute of Technology and Stockholm University).

KRAEMER, S. and CARAYON, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics,* **38** (2), 143-154.

KSHETRI, N. (2007). Barriers to e-commerce and competitive business models in developing countries: A case study. *Electronic commerce research and applications,* **6** (4), 443-452.

LEE, P. M. (2002). Behavioral model of online purchasers in e-commerce environment. *Electronic commerce research,* **2** (1), 75-85.

LEE, T. (1999). *Using qualitative methods in organizational research.* London, SAGE.

LEE, Y., LEE, J. and LEE, Z. (2002). Integrating software lifecycle process standards with security engineering. *Computers & security,* **21** (4), 345-355.

LEGARD, R., KEEGAN, J. and WARD, K. (2003). In-depth interviews. In: *Qualitative research practice.* Ritchie, J.; Lewis, J ed., London, SAGE, .

LEWIN, K. (1951). *Field theory in social science.* New York, Harper & Bros.

LI, F. (2007). *What is E-business?: How the internet transforms organisations.* Blackwell Publishing.

LINCOLN, Y. S. and GUBA, E. G. (1985). *Naturalistic inquiry.* London, SAGE.

LONGSTAFF, T., et al. (1997). Security of the internet. *The Froehlich/Kent encyclopedia of telecommunications,* **15** , 231-255.

LUBORSKY, M. and RUBINSTEIN, R. (1995). Sampling in qualitative research: Rationale, issues, and methods. *Research on aging,* **17** (1), 89.

MARSHALL, C. and ROSSMAN, G. (1999). *Designing qualitative research.* Sage Publications. London, UK.

MARSHALL, M. (1996). Sampling for qualitative research. *Family practice,* **13** , 522-525.

MCCOLE, P., RAMSEY, E. and WILLIAMS, J. (2009). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of business research,* .

MCCONNELL (2002). *The national E-readiness of the Hashemite kingdom of Jordan: A global view of Jordan's competitive advantages.* McConnell International.

MCCONNELL (2005). *Cyber crimes and punishments, archaic laws threaten global information.* McConnell International.

MCCROHAN, K. F. (2003). Facing the threats to electronic commerce. *Journal of business & industrial marketing,* **18** (2), 133-145.

MCGRAW, G. (2004). Software security. *Security & privacy, IEEE,* **2; 2** (2), 80-83.

MENAFN (2008). Jordan's private, public sectors partnership - a new concept: *MENAFN,* .

MEYERS, M. and AVISON, D. (2002). *Qualitative research in information systems: A reader.* London, SAGE Publications.

MILES, M. B. and HUBERMAN, A. M. (1994). *Qualitative data analysis: An expanded sourcebook.* 2nd ed., Sage Pubns.

MIYAZAKI, A. D. and FERNANDEZ, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of public policy & marketing,* , 54-61.

MOCKLER, R., DOLOGIT, D. and GARTENFELD, M. (2008). B2B E-business. *Electronic commerce: Concepts, methodologies, tools and applications,* , 9.

MoICT (2008). *Jordan national e-commerce strategy 2008-2012.* [online]. Jordan, Ministry of Information and Communication Technology (MoICT). at: http://www.moict.gov.jo/MoICT_National_E-Commerce_Strategy.aspx.

MOLLA, A. and LICKER, P. S. (2005). Perceived e-readiness factors in e-commerce adoption: An empirical investigation in a developing country. *International journal of electronic commerce,* **10** (1), 83-110.

MOURATIDIS, H., GIORGINI, P. and MANSON, G. (2005). When security meets software engineering: A case of modelling secure information systems. *Information systems,* **30** (8), 609-629.

MYERS, M. (1997). Qualitative research in information systems. *MIS quarterly,* , 241-242.

NABI, F. (2005). Secure business application logic for e-commerce systems. *Computers & security,* **24** (3), 208-217.

NEWMAN, I., et al. (2003). A typology of research purposes and its relationship to mixed methods. In: TASHAKKORI, A., TEDDLIE, C. and THOUSAND OAKS, C. (eds.). *Handbook of mixed methods in social and behavioral research.* London, SAGE, 167-188.

NGAI, E. and WAT, F. (2002). A literature review and classification of electronic commerce research. *Information & management,* **39** (5), 415-429.

OATES, B. (2006). *Researching information systems and computing.* London, Sage.

OBEIDAT, M. (2001). Consumer protection and electronic commerce in Jordan (an exploratory study). In: *Organization for Economic Cooperation and Development Conference on Electronic Commerce,* 2001. The Public Voice, .

ODLYZKO, A. (2003). Economics, psychology, and sociology of security. *Lecture notes in computer science,* , 182-189.

OpenNet (2009). *Internet filtering in Jordan.* [online]. OpenNet initiative. at: http://opennet.net/research/profiles/jordan.

ORLIKOWSKI, W. (1993). CASE tools as organizational change: Investigating incremental and radical changes in systems development. *MIS quarterly,* , 309-340.

ORLIKOWSKI, W. and BAROUDI, J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information systems research,* **2** (1), 1-28.

OTUTEYE, E. (2003). A systematic approach to e-business security.

PAHLADSINGH, S. (2006). *Barriers to effective e-business.* [online]. Last accessed 09/11 2009 at: www.emarketservices.com.

PAINE, Carina, et al. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International journal of human-computer studies,* **65** (6), 526-536.

PAPAZAFEIROPOULOU, A., POULOUDI, A. and CURRIE, W. (2001). Applying the stakeholder concept to electronic commerce: Extending previous research to guide government policy makers. In: *PROCEEDINGS OF THE ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES,* 122-122.

PAPAZOGLOU, M. and RIBBERS, M. (2006). e-business: Organizational and technical foundations.

PFLEEGER, C. and PFLEEGER, S. (2003). *Security in computing.* 3rd ed., USA, Prentice Hall.

PHILLIPS, R., FREEMAN, R. and WICKS, A. (2003). What stakeholder theory is not. *Business ethics quarterly,* **13** (4), 479-502.

PONS, A., ALJIFRI, H. and FOURATI, K. (2003). E-commerce and Arab intra-trade. *Information technology & people,* **16** (1), 34-48.

POPE, C., ZIEBLAND, S. and MAYS, N. (2000). Qualitative research in health care: Analysing qualitative data. *British medical journal,* **320** (7227), 114.

POSTHUMUS, S. and VON SOLMS, R. (2006). A responsibility framework for information security. *IFIP international federation for information processing,* **Volume 193/2006** .

POULOUDI, A. (1999). Aspects of the stakeholder concept and their implications for information systems development. In: *PROCEEDINGS OF THE HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES,* Citeseer, 254-254.

POULOUDI, A. and WHITLEY, E. (1997). Stakeholder identification in inter-organizational systems: Gaining insights for drug use management systems. *European journal of information systems,* **6** (1), 1-14.

PRANANTO, A., MCKAY, J. and MARSHALL, P. (2001). Frameworks to support e-business growth strategy. *Proceedings of the global cooperation in the new millenium, ECIS,* , 1254-1263.

PRIVACY INTERNATIONAL (2007). *PHR2006 - the Hashemite kingdom of Jordan.* UK, Privacy International.

QTEISHAT, M. (2010). *Evaluation stakeholders attitudes to ICT in adoption of E-learning in Jordan.* PhD. Sheffield Hallam University.

REDING, V. (2007). Enhanced information security in software and services: What role for government, security providers and users? In: *European Information Security Awareness Day Speech,* .

RITCHIE, J. and SPENCER, L. (1994). Qualitative data analysis for applied policy research. In: BRYMAN, A. and BURGESS, R. (eds.). *Analysing qualitative data.* London, Routledge, 173–194.

RITCHIE, J., SPENCER, L. and O'CONNOR, W. (2003). Carrying out qualitative analysis. In: RITCHIE, J. and LEWIS, J. (eds.). *Qualitative research practice: A guide for social science students and researchers.* London, SAGE, 219-262.

RJ (2005). *Royal Jordanian annual report.* [online]. at: http://www.rj.com/pdf/annual_report/RJ_Annual_Report_2005.pdf.

RJ (2006). *Royal Jordanian annual report.* [online]. at: http://www.rj.com/pdf/annual_report/RJ%202006%20e.pdf.

RJ (2007). *Royal Jordanian annual report.* [online]. at: http://www.rj.com/pdf/RJ_Annual_Report_2007.pdf.

RJ (2008). *Royal Jordanian annual report.* [online]. at: http://www.rj.com/pdf/annual_report/RJ_Annual_Report_2008.pdf.

RJ news (2006a). *New RJ website to offer expanded services.* [online]. at: http://www.rj.com/about_rj/article_300506.asp.

RJ news (2006b). *RJ introduces Tejari's e-procurement system.* [online]. at: http://www.rj.com/about_rj/article_210806.asp.

RJ news (2006c). *Royal Jordanian partners with Lufthansa systems to optimize revenue accounting.* [online]. at: http://www.rj.com/about_rj/article_250206.asp.

RODGERS, J., YEN, D. and CHOU, D. (2002). Developing e-business: A strategic approach. *Information management and computer security,* **10** (4), 184-192.

ROGERS, E. (1995). *Diffusion of innovations.* Free press.

RUDESTAM, K. and NEWTON, R. (2007). *Surviving your dissertation: A comprehensive guide to content and process.* 3rd ed., SAGE-UK.

RYAN, F., COUGHLAN, M. and CRONIN, P. (2007). Step-by-step guide to critiquing research. part 2: Qualitative research. *British journal of nursing,* **16** (12), 738-744.

SALISBURY, W. D., et al. (2001). Perceived security and world wide web purchase intention. *Industrial management and data systems,* **101** (3), 165-176.

SANDERS, N. (2007). An empirical study of the impact of e-business technologies on organizational collaboration and performance. *Journal of operations management,* **25** (6), 1332-1347.

SANS Institute (2009). SANS top 20 vulnerabilities.

SCHNEIER, B. (2004). *Secrets and lies: Digital security in a networked world.* Wiley New York.

SCHNEIER, B. (2006). *Do federal security regulations help?* [online]. Last accessed 02/15 2006 at: http://www.schneier.com/essay-141.html.

SCHNEIER, B. (2008). The psychology of security. *Lecture notes in computer science,* , 50-79.

SCOTT, J. (2004). Measuring dimensions of perceived e-business risks. *Information systems and e-business management,* **2** (1), 31-55.

SEAMAN, C. (1999). Qualitative methods in empirical studies of software engineering. *IEEE transactions on software engineering,* **25** (4), 557-572.

SHANKAR, V., URBAN, G. and SULTAN, F. (2002). Online trust: A stakeholder perspective, concepts, implications, and future directions. *Journal of strategic information systems,* **11** (3-4), 325-344.

SHANKAR, V., URBAN, G. L. and SULTAN, F. (2002). Online trust: A stakeholder perspective, concepts, implications, and future directions. *Journal of strategic information systems,* **11** (3-4), 325-344.

SIDDIQI, J., ALQATAWNA, J. and HJOUJ BTOUSH, M. (2010). Do insecure systems increase global digital divide? Book chapter in: KAMEL, S. (ed.). *Strategies for technological diffusion and Adoption: National ICT Approaches for socioeconomic development.* IGI Global.

SIDDIQI, J., et al. (2002). E-commerce: Continuous growth or leveling out? In: *Proceedings of the International Conference on Information Technology,* 491-497.

SIPONEN, M. (2005a). An analysis of the traditional IS security approaches: Implications for research and practice. *European journal of information systems,* **14** (3), 303-315.

SIPONEN, M. (2005b). Analysis of modern IS security development approaches: Towards the next generation of social and adaptable ISS methods. *Information and Organization,* **15** (4), 339-375.

SIPONEN, M. and OINAS-KUKKONEN, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS database,* **38** (1), 80.

SLEWE, T. and HOOGENBOOM, M. (2004). Who will rob you ON THE DIGITAL HIGHWAY? *Communications of the ACM,* **47** (5), 56.

SMITH, B., et al. (eds.) (2001). *iSeries e-business handbook.* 2nd ed., IBM Corporation.

SRINIVASAN, S. (2004). Role of trust in e-business success. *Information management and computer security,* **12** , 66-72.

STAKE, R. (1995). *The art of case study research: Perspectives on practice.* London, SAGE.

STALLINGS, W. (1998). *Cryptography and network security: Principles and practice.* Upper Saddle River, NJ: Prentice Hall.

STENSGAARD, A. (2006). Al quds college graduates to e-commerce with Tejari. *AMEinfo,* .

STRAUB JR, D. W. (1990). Effective IS security: An empirical study. *Information systems research,* **1** (3), 255-276.

STRAUB, D., GEFEN, D. and BOUDREAU, M. (2004). *The isworld quantitative, positivist research methods website.* [online]. Last accessed 1/20 2010 at: http://dstraub.cis.gsu.edu:88/quant/2philo.asp.

STRAUB, D. W. and WELKE, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS quarterly,* , 441-469.

STRAUSS, A. and CORBIN, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques.* Newbury Park, CA, SAGE.

SUH, B. & HAN, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International journal of electronic commerce,* 7 (3), 135-161.

SUH, B. and HAN, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International journal of electronic commerce,* 7 (3), 135-161.

SUNDT, C. (2006). Information security and the law. *Information security technical report,* **11** (1), 2-9.

TARIMO, C. (2006). *ICT security readiness checklist for developing countries: A social-technical approach.* PhD. Department of Computer and Systems Sciences, Stockholm University.

THOMAS, D. (2006). A general inductive approach for qualitative data analysis. *American journal of evaluation,* **27** (2), 237-246.

TITI, K. (2005). The impact of adoption electronic commerce in small to medium enterprises Jordanian companies. In: *Proceeding of the 1st International Conference on e-Business and e-Learning,* 159-178.

TRACY, K. (2000). What's the deal with "e-business"? *IEEE potentials,* **19** (1), 34-35.

TRAUTH, E. (2001). The choice of qualitative methods in IS research. In: *Qualitative research in IS: Issues and trends.* Trauth, E. ed., London, Idea Group, 1-19.

TRIST, E. and BAMFORTH, K. (1951). Some social and psychological consequences of the longwall method of coal-getting: An examination of the psychological situation and defences of a work group in relation to the social structure and technological content of the work system. *Human relations,* **4** (1), 3.

TSIAKIS, Theodosios and STHEPHANIDES, George (2005). The concept of security and trust in electronic payments. *Computers & security, elsevier ltd,* **24** (1), 10-15.

TSUJII, S. (2004). Paradigm of information security as interdisciplinary comprehensive science. In: *Proc. of the 2004 International Conference on Cyberworlds (CW'04), IEEE Computer Society,* 1-12.

TURBAN, E., et al. (2008). *Electronic commerce 2008: A managerial perspective.* Pearson, Prentice Hall.

TURNER, C. (2003). How do consumers form their judgments of the security of e-commerce web sites. In: *ACM/CHI2003 Workshop on Human-Computer Interaction and Security Systems,* .

UDO, G. (2001). Privacy and security concerns as major barriers for e-commerce: A survey study. *Information management and computer security,* **9** (4), 165-174.

UK national statistics: E-security. (2005). [online]. Last accessed 01/20/2008 at: http://www.statistics.gov.uk/cci/nugget.asp?id=1717.

UN-ESCWA (2007). *Regional profile of the information society.* [online]. Last accessed 08/17/2009 at: http://isper.escwa.org.lb/isper/Default.aspx?tabid=142&language=en-US.

VON SOLMS, B. (2000). Information Security—The third wave? *Computers & security,* **19** (7), 615-620.

VON SOLMS, B. and VON SOLMS, R. (2004). The 10 deadly sins of information security management. *Computers & security,* **23** (5), 371-376.

WALSHAM, G. (1993). *Interpreting information systems in organizations.* Chichester, UK, Wiley.

WALSHAM, G. (1995). The emergence of interpretivism in IS research. *Information systems research,* **6** (4), 376-394.

WALSHAM, G. (2006). Doing interpretive research. *European journal of information systems,* **15** (3), 320-330.

WANG, G. (2005). Strategies and influence for information security. *INFORMATION SYSTEMS CONTROL JOURNAL,* **1** .

WAREHAM, J., ZHENG, J. and STRAUB, D. (2005). Critical themes in electronic commerce research: A meta-analysis. *Journal of information technology,* **20** (1), 1-19.

WEILL, P. and VITALE, M. (2002). What IT infrastructure capabilities are needed to implement e-business models. *MIS quarterly executive,* **1** (1), 17-34.

WENNINGER, J. and LUSTSIK, O. (2000). The emerging role of banks in e-commerce. *Current issues in economics and finance,* **6** (3).

WERLINGER, R., et al. (2009). Security practitioners in context: Their activities and interactions with other stakeholders within organizations. *International journal of human-computer studies,* .

WILLIAMS, N. (2003). E-business security issues for SMEs in a virtual hosting environment. In: *Proceedings of the 1st International Symposium on Information and Communication Technologies,* Trinity College Dublin, 364.

WILSON, B. (1990). *Systems: Concepts, methodologies, and applications.* New York, NY, USA, John Wiley & Sons.

WIMMER, M. and VON BREDOW, B. (2002). A holistic approach for providing security solutions in e-government. In: *Proceedings of the 35th Hawaii International Conference on System Sciences,* 1715-1724.

WINDRUM, P. and BERRANGER, P. (2004). Factors affecting the adoption of intranets and extranets by SMEs: A UK study. In: *Innovation through Information Technology,* New Orleans, Idea Gruop, .

WORLD ECONOMIC FORUM (2009). *Global information technology report 2008- 2009: Mobility in a networked world.*

WYMER, S. and REGAN, E. (2005). Factors influencing e-commerce adoption and use by small and medium businesses. *Electronic markets,* **15** (4), 438-453.

YASIN, M. M. and YAVAS, U. (2007). An analysis of E-business practices in the Arab culture. *International journal,* **14** (1), 68-73.

YASIN, M. M. and YAVAS, U. (2007). An analysis of E-business practices in the arab culture: Current inhibitors and future strategies. *Cross cultural management: An international journal,* **14** (1), 68-73.

YIN, R. (2003). *Case study research: Design and methods.* London, SAGE.

YNGSTRÖM, L. (1996). *A systemic-holistic approach to academic programmes in IT security.* PhD. Department of Computer and Systems Sciences (Stockholm University and Royal Institute of Technology).

YNGSTROM, L. and BJORCK, F. (1999). The value of assessment of information security education and training. In: *Proceedings of WISE1 - First World Conference on Information Security Education,* Citeseer, 271-292.

ZAKARIA, O. (2004). Understanding challenges of information security culture: A methodological issue. In: *2nd Australian Information Security Management Conference,* Citeseer, 83.

ZAKARIA, O. (2007). *Investigating information security culture challenges in a public sector organisation: A Malaysian case.* PhD. University of London.

ZIPKIN, D. (2005). *Using STAMP to understand recent increases in malicious software activity.* MSc. Massachusetts Institute of Technology.

ZUCCATO, A. (2007). Holistic security management framework applied in electronic commerce. *Computers & security,* 26 (3), 256-265.

ZURKO, M. E. and SIMON, R. T. (1996). User-centered security. In: *Proceedings of the 1996 Workshop on New Security Paradigms,* ACM New York, NY, USA, 27-33.

Appendix A: Topic guides used in the case study protocol

Technology Providers Semi-Structured Interview Guide:

This interview aims to explore the perspective of technology providers in respect to e-Business security in the context of the study. Representative respondents from several technology providers (hardware providers, software providers, ISPs, web-hosting companies, etc.) in the study environment will be interviewed.

General Theme:

1. Could you please provide an overview of the services or product that you provide to e-Business companies in Jordan?
2. What is your core business?
3. How long have you been in the market?
4. How many Employees do you have?
5. Who are your target customers?

Semi-structured Interview Guide

1. In your opinion as a technology vendor/provider, what are the critical success factors for e-Business in Jordan?
2. What are the main features of your products/services that you always make sure to provide to your e-Business customers? (Probe: What about security - if not mentioned - ?)
3. What do customers usually ask for in e-Business infrastructure?
   (Probe: What about security - if not mentioned- ?)
4. Do you think security is important at this early stage of e-Business diffusion in Jordan? Why?
5. In your opinion, who is responsible for the security of e-Business?
6. What do technology vendors/providers offer in respect to e-Business security? (In other words, what is the role of the technology vendors/providers in this matter? Are they fulfilling this role?)
7. How do you make sure that the products/services that you offer provide adequate security for your e-Business customers?
8. Who is liable for security breaches which result from product/services?
9. What are the factors that contribute to increase trust in the e-Business environment in Jordan?
10. What do you think is the role of the government in respect to e-Business security in Jordan?
11. Is there any public-private sector partnership concerning security of e-Business environment in Jordan?

E-Business Organisations Semi-Structured Interview Guide:

Site Overview

e-Business Organisation General Theme:

This theme aims to explore general information about e-Business activities and can be filled in by any one who represents the e-Business organisation under investigation.

1. Describe your organisation's e-Business modes (select all appropriates):
   A. Business-to-Customers (B2C).
   B. Business-to-Business (B2B).

2. 2.1 Describe you infrastructure (select all appropriate):

   A. Intranet.
   B. Internet.
   C. Virtual Private Network (VPN).

   2.2 List - if any - activities or services(for example security, payment, web hosting, IT helpdesk) that you outsource:
   .....
   .....
   .....

3. Describe your organisation's e-Business activities(select all appropriate):

   A. Selling over the Internet.
   B. Buying over the Internet.
   C. Provide customers with e-services (e-bills, placing orders, tracing orders,..etc.)
   D. Collaboration with business partners over ICT infrastructure.
   E. Processing financial or personal information over ICT infrastructure.
   F. Other activities. Please specify:.....

4. Do you have any of the following e-Business applications? (select all appropriate):

   A. Customer Relationship Management (CRM).
   B. Enterprise Resource Planning (ERP).
   C. e-Procurement.
   D. Supply Chain Management (SCM).
   E. Change Management System.
   F. Asset Management System.
   G. Other:.....

Management Interview Guide

This guide contains the possible Themes/Questions/Issues that the researcher can use to explore management perceptions regarding e-Business security. Potential respondents: any one in a management position (CEO, CIO, CSO, CFO...etc).

1. In your opinion, what are the critical success factors for e-Business?
2. What are the main issues that faced your organisation when you decided to provide business over the Internet?
3. What are the factors that affect your trust in the digital environment?
4. What do you do to increase customers' trust and encourage them to use your online services?
5. What does security of e-Business means for you?
6. How is security incorporated in your e-Business activities?
7. Who is responsible for e-Business security at your organisation?
8. How does board of directors/top management contribute to e-Business security in your organisation?
9. How do you ensure that your employees are aware of their responsibility in respect to e-Business security? (Probe: what about background check, rewards, motivation, punishment and communication of security related responsibilities through training and awareness).
10. What are the factors that you consider when you assign a budget for IT security?
11. If third-party vendors are hosting/maintaining critical applications/information, what provisions are in place contractually to insure against loss or privacy violation?
12. How do you promote security for your online customers? (Probe: encourage customer to follow some security practices, security as competitive advantage).
13. What is the reference source in your organisation about what is allowed and what is not allowed in relation to electronic information processing? Who devises these rules?
14. What ICT standards or best practices do you have in place for efficient/secure business practices? (Probe: was this your own choice or you are forced to comply with this by the government or any regulatory body?)
15. In your opinion, how can the government help in providing secure e-Business?
16. How do you establish trust relations with your technology providers? What affects these relations?
17. How does the existing legislation and regulatory bodies' practices (positively/negatively) affect your feeling of trust in the digital environment?

Technical Staff Interview Guide

This guide contains the possible Themes/Questions/Issues that the researcher can use to explore IT staff perceptions regarding e-Business security. Potential respondents: any one from the site technical team (Systems Admin, Network Admin, Programmer...etc).

1. To what extent does your organisation depends on the electronic processing, storage and transmission of information?
2. What are the main things that came to your mind when your organisation decided to provide e-services through the Internet? (Probe: how does security come into the picture)
3. What are the consequences of having information unavailable, inaccurate or accessible by unauthorised persons?
4. How does your organisation ensure secure processing, storage and transmission for the information?
5. How does your organisation control the physical security of its ICT infrastructure?
6. In your opinion, what is the main security threat that your e-Business may face? And how is your organisation dealing with that?
7. In the case of any e-Business initiative, how does your organisation determine its security requirements? Who usually participates in this process?
8. How does the technical staff learn about information security? (Probe: do you have a dedicated security engineer?)
9. Who is responsible for the security incidents and to whom he should report? (Probe: who is the main person responsible for security?)
10. What factors did you consider when you designed your website in order to make the customer feel comfortable and safe and to minimize the chance or error that may lead to security breaches?
11. What is the reference source in your organisation about what is allowed and what is not allowed in relation to electronic information processing? Who devises these rules? How are they enforced?

Employees Interview Guide

This guide contains the possible Themes/Questions/Issues that the researcher can use to explore employees' perceptions regarding e-Business security. Potential respondents: any employee who is neither technical nor in a management position.

1. You leave your desk/office for a short or long time, are there any particular things you make sure to do before leaving?
2. If you are at home and there is a file that you stored in your computer at work and you need this file what will you do to get this file?
3. What does e-Business security means for you?
4. Do you use one password to use everywhere in the Internet or login to PC at work? How do you recall this/these password(s)?
5. Do you follow any particular procedure for creating your password?
6. Do you think that the management has the right to monitor its employees? Why?
7. Have you signed or agreed on any thing related to maintain the security of the company information? Do you think people are very committed to such things? Why?
8. If you are not sure if downloading some software/attachment or accessing particular websites could cause some security problems what will you do?
9. What do you do to protect yourself from security related incidents while surfing the internet or checking your e-mail during your work? Where have you got such knowledge?
10. What the do you think the term "Social Engineering" is related to or means?
11. In your opinion, who is responsible for e-Business security in your organisation?

Legal Interview Guide

This guide contains the possible Themes/Questions/Issues that the researcher can use to explore the e-business organisation perceptions regarding legal issues related to e-Business security. These questions can be asked of the legal department

1. What are the legal requirements or regulations that affect your e-Business?
2. How do you make sure that your organisation is "aware" of these various legal rules and regulations regarding e-Business?
3. How do you guarantee that any online transaction is completely accurate and legally binding?
4. How do you ensure that any online transaction is completely accurate and legally binding?
5. How do you collect digital evidence related to online transactions? Are these digital evidences acceptable in the court?
6. What ICT standards or best practices do you have in place for efficient/secure business practices? (Probe: was this your own choice or you are forced to comply with this by the government or any regulatory body?)
7. From a legal point of view, what does e-Business security means for you?
8. How do the digital crimes affect e-Business?
9. In your opinion, how can government help in providing secure e-Business?
10. Do you think that the current legal framework is strong enough to provide a secure e-Business environment? Why?

Online Customer Semi-Structured Interview guide

The aim of this interview is to explore customers' perceptions in respect to e-Business security. It has three themes: Customers' Online Security Attitudes and Behaviours; Customer's Security Education and Awareness; and Customers' Security Expectations.

Online Customer General Theme:

This theme aims to explore general information about online customers' activities.

5. Customer general information:
    A. Age_____
    B. Gender_____
    C. Current status (student, employee...etc.)_____
    D. Educational background_____
    E. Your e-mail (for future communication)_____
6. Describe your Internet activities (select all applicable):
    A. Selling over the Internet.
    B. Buying over the Internet.
    C. Online banking.
    D. e-Billing.

E. Communication with other using VOIP, IM, e-mail or online social networks.
F. Other activities. Please specify:.....

7. How long have you been an Internet user:_____
8. Do you own any of the following cards (select all applicable):
   A. Credit cards.
   B. Debit cards.
   C. Internet shopping cards.

1. Do you think that buying/selling over the Internet is a good thing? Why?
2. What do you think the advantage/disadvantage of online shopping compare to face-face shopping?
3. What are the things that affect your decision to engage in e-commence transaction?
4. How do you feel when you give any personal information online? Why?
5. Do you think that the Internet is risky? Why?
6. What does security mean for you?
7. In your opinion, who is responsible for providing secure online environment? Why?
8. What do you do to protect your self while surfing/transacting over the Internet?
9. In General, do you trust technology? Why?
10. Do you think that you have the capability to protect your online security? Why?
11. Can you mention some online threats that might violate your online security?
12. What security features/tools are there in your PC to increase your security and protect your privacy while surfing the Internet?
13. Do you use one password everywhere on the Internet or login to PC at work/School? How do you recall this/these password(s)? 14. (Probe: Do you follow any particular procedure for creating your password?)
15. How do you deal with e-mails that you receive from unknown sources?
16. What does privacy mean for you?
17. What does each of the following terms mean? a. HTTPS, b. SSL, c. Digital Certificate, d. Privacy Policy, e. Encryption, f. Secure Website. g. Phishing.
18. How do you deal with websites that ask you to download and execute some files to complete their transactions? Why?
19. Have you ever received any information security related education or training? If yes, where?
20. What factors contribute to increase your trust in e-Business in Jordan?
21. What do you think companies should do to protect customers' online security and privacy?
22. What do you think is the role of the government in this matter? Probe: How can the government contribute to providing customers with a secure online environment? Probe: Currently, do they really have an effective role in that?