PhD Thesis

Investigating the Factors that Influence the Effectiveness of E-Commerce Security (A Jordanian Context)

Mohanad Ali Halaweh

CCSR
Faculty of Technology
(Computing Science and Engineering)
De Montfort University, United Kingdom

Submitted in partial fulfilment of the requirements for the

De Montfort University
Degree of Doctor of Philosophy
March 2009
Abstract

Of all the factors restricting their engagement and participation in e-commerce, security is the main concern for customers and businesses alike. Existing research has dealt with the issue of e-commerce security by focusing separately on the customer or on the business, but there is little research attempting to investigate both as a single phenomenon. This research considers the two perspectives jointly in order to establish a comprehensive viewpoint, and to reduce the gap between the solutions and security being implemented by organisations, on the one hand, and the perceptions of customers, on the other hand, thus allowing a more in-depth understanding of the customer’s needs and priorities to be taken into account by organisations. This research is undertaken in Jordan, an environment where no other research into security perception in e-commerce has taken place. The reason for choosing the Jordanian context is justifiable as most existing research conducted in Jordan confirms the security concern in e-commerce and Internet banking, without exploring the issue in depth. This barrier (i.e. security) makes both Jordanian organisations and individual customers hesitant to participate in e-commerce transactions, and thus reduces the growth of e-commerce. An interpretive case study method has been adopted and guides the grounded theory analysis method of research into the perceptions of customers and of businesses and IT personnel. This research, which is qualitative and subjective in nature, involves examining and identifying the meanings of the participants in order to gain an understanding of the phenomenon under study. Qualitative research enables the researcher to understand the phenomenon in depth without being limited to certain predetermined hypothesis and factors that are defined from literature, so that issues are allowed to emerge from the natural setting of the context (i.e. Jordan). Grounded theory procedures and techniques have been used to explore the relevant influence of factors on the effectiveness of e-commerce security and to identify the relationships between them. The empirical findings show seven factors: cooperative responsibility, implementation concerns, commitment of management, users’ characteristics, social communication, psychological aspect of security, and tangible and intangible features of security. Finally, a critical discussion of research implications has been drawn which extends the theoretical base of e-commerce security within the IS domain and provides broad insight for decision-makers and practitioners in Jordan.
Acknowledgment

First of all, I would like to thank God for all his blessings and guidance.

I would like to express my sincere gratitude to my parents, brothers and sisters. Without their continuous encouragement and support, the successful completion of this project would never have been possible.

I am very grateful to my supervisor, Dr Christine Fidler, as without her excellent guidance, this work would not have completed. She has provided me with valuable advice and support. I would like to thank her for tolerantly reading through my draft chapters and thesis, and for her encouragement to publish papers. I would also like to thank Mr Steve McRobb, my second supervisor, for his critical remarks throughout the course of this research, and for his review of the thesis.

A thank you also goes to the transfer assessor for this thesis, Dr Bernd Stahl, for his advice in the early stages of my research, and for his organisation of the biweekly ISDP seminar in the school of Computing at De Montfort University. This provided me with excellent guidelines, regarding IS research paradigms and methods, at an early stage of my research; this enabled me to present and discuss my research with other scholars and PhD students in the school.

Finally, I would also like to thank all respondents who participated in this research; without them, the empirical data would not have been produced.

Mohanad Halaweh
March 2009.
Publications

Refereed Papers published by the author from this thesis. Full Papers are attached in appendix E.


### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS</td>
<td>Information Systems</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ICT</td>
<td>Information Communication and Technology</td>
</tr>
<tr>
<td>B2B</td>
<td>Business to Business</td>
</tr>
<tr>
<td>B2C</td>
<td>Business to Customer</td>
</tr>
<tr>
<td>C2C</td>
<td>Customer to Customer</td>
</tr>
<tr>
<td>B2E</td>
<td>Business to Employee</td>
</tr>
<tr>
<td>G2C</td>
<td>Government to Customer</td>
</tr>
<tr>
<td>G2B</td>
<td>Government to Business</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>EIC</td>
<td>E-commerce Information Center</td>
</tr>
<tr>
<td>INTAJ</td>
<td>Information Technology Association of Jordan</td>
</tr>
<tr>
<td>ICDL</td>
<td>International Computer Driving Licence</td>
</tr>
<tr>
<td>EBDA</td>
<td>Electronic Business Development Activity</td>
</tr>
<tr>
<td>ACI</td>
<td>Amman Chamber of Industry</td>
</tr>
<tr>
<td>WIPO</td>
<td>World Intellectual Property Organisation</td>
</tr>
<tr>
<td>SME</td>
<td>Small Medium Enterprise</td>
</tr>
<tr>
<td>JCC</td>
<td>Jordan Chamber of Commerce</td>
</tr>
<tr>
<td>NGO</td>
<td>Non-Governmental Organization</td>
</tr>
<tr>
<td>GT</td>
<td>Grounded Theory</td>
</tr>
<tr>
<td>QDA</td>
<td>Qualitative Data Analysis</td>
</tr>
<tr>
<td>GTM</td>
<td>Grounded Theory Methodology</td>
</tr>
<tr>
<td>EPS</td>
<td>Electronic Payment System</td>
</tr>
<tr>
<td>EPG</td>
<td>Electronic Payment Gateway</td>
</tr>
<tr>
<td>PCI</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
</tbody>
</table>
# Table of Contents

Abstract ........................................................................................................................................... ii  
Acknowledgment ........................................................................................................................... iii  
Publications .................................................................................................................................... iv  
Abbreviations ................................................................................................................................... v  
Table of Contents ............................................................................................................................. vi  
List of Figures and Tables .................................................................................................................. ix  

Figure 6.11 Factors that influence on e-commerce security effectiveness from the organization perspective ................................................................. ix  

Chapter 1: Introduction .................................................................................................................... 1  
1.1 Introduction .................................................................................................................................. 1  
1.2 Information Security Surveys ........................................................................................................ 2  
1.3 Motivation ..................................................................................................................................... 4  
1.4 Objectives .................................................................................................................................... 5  
1.5 Research Questions ...................................................................................................................... 5  
1.6 Organisation of the Thesis ........................................................................................................... 6  

Chapter 2: Literature Review .......................................................................................................... 8  
2.1 Definition and overview of E-commerce ...................................................................................... 8  
2.2 E-commerce categories ............................................................................................................... 9  
2.3 Participants in E-commerce ........................................................................................................ 10  
2.4 Benefits of and barriers to E-commerce ..................................................................................... 11  
2.5 Definition of IS Security ............................................................................................................ 12  
2.6 Information and E-commerce Security Requirements .............................................................. 13  
2.7 Security Models in E-commerce ............................................................................................... 18  
2.8 Customer’s security perceptions ............................................................................................... 25  
2.9 Analysis of Existing Frameworks ............................................................................................... 30  
2.10 Implications of the Analysis ....................................................................................................... 34  
2.11 Proposed Research Model ......................................................................................................... 35  
2.12 ICT and E-commerce in Jordan ............................................................................................... 36  
2.12.1 General information about Jordan ..................................................................................... 37  
2.12.2 ICT development in Jordan ............................................................................................... 37  
2.12.3 Previous e-commerce studies in Jordan ............................................................................. 41  
2.13 Summary and Conclusion ......................................................................................................... 43  

Chapter 3: Research Methodology ................................................................................................ 44  
3.1 Research Paradigm ..................................................................................................................... 45  
3.1.1 Positivist Paradigm ................................................................................................................. 45  
3.1.2 Interpretive Paradigm .............................................................................................................. 46  
3.1.3 Critical Paradigm .................................................................................................................... 47  
3.2 Research paradigms in IS Security ............................................................................................. 49  
3.2.1 Positivist paradigm in IS Security ....................................................................................... 50  
3.2.2 Interpretive paradigm in IS Security .................................................................................... 51  
3.3. Research methods ..................................................................................................................... 52  
3.4 Case Study research .................................................................................................................... 55  
3.4.1 Design of the case study research ....................................................................................... 56  
3.4.2 Criticisms of case studies ...................................................................................................... 58  
3.5 Justification for selected research paradigm and method .......................................................... 59
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.6 Conclusion</td>
<td>61</td>
</tr>
<tr>
<td>Chapter 4: Using Grounded Theory for Data Analysis</td>
<td>61</td>
</tr>
<tr>
<td>4.1 Grounded Theory Overview</td>
<td>62</td>
</tr>
<tr>
<td>4.2 Grounded Theory Approaches</td>
<td>62</td>
</tr>
<tr>
<td>4.3 Grounded Theory Procedures</td>
<td>65</td>
</tr>
<tr>
<td>4.4 Justification for using grounded theory and in particular the Straussian approach with case study research method</td>
<td>68</td>
</tr>
<tr>
<td>4.5 Criteria for evaluating the quality of research design</td>
<td>71</td>
</tr>
<tr>
<td>4.6 Conclusion</td>
<td>73</td>
</tr>
<tr>
<td>Chapter 5: Data Collection Process</td>
<td>74</td>
</tr>
<tr>
<td>5.1 Selection of the case studies</td>
<td>75</td>
</tr>
<tr>
<td>5.2 Ethical considerations</td>
<td>76</td>
</tr>
<tr>
<td>5.2 Case study protocol</td>
<td>81</td>
</tr>
<tr>
<td>5.3 The rationale for the use of the initial model and the case study protocol</td>
<td>80</td>
</tr>
<tr>
<td>5.4 Beginning the Fieldwork</td>
<td>81</td>
</tr>
<tr>
<td>5.5 Data Saturation</td>
<td>82</td>
</tr>
<tr>
<td>5.6 Conclusion</td>
<td>83</td>
</tr>
<tr>
<td>Chapter 6: Data Analysis</td>
<td>83</td>
</tr>
<tr>
<td>6.1 Application of grounded theory procedures</td>
<td>84</td>
</tr>
<tr>
<td>6.2 Results of analysis based on the customer perspective</td>
<td>86</td>
</tr>
<tr>
<td>6.2.1 User’s/Customers Characteristics</td>
<td>86</td>
</tr>
<tr>
<td>6.2.2 Security meanings and needs</td>
<td>89</td>
</tr>
<tr>
<td>6.2.3 Tangible and intangible indicators of security</td>
<td>90</td>
</tr>
<tr>
<td>6.2.4 Psychological aspect of security</td>
<td>95</td>
</tr>
<tr>
<td>6.2.5 Cooperative Responsibility</td>
<td>98</td>
</tr>
<tr>
<td>6.3 Results of analysis from the organisational perspective</td>
<td>100</td>
</tr>
<tr>
<td>6.3.1 The customer’s concerns regarding security and e-commerce from an organisational viewpoint</td>
<td>101</td>
</tr>
<tr>
<td>6.3.2 Psychological aspect of security</td>
<td>104</td>
</tr>
<tr>
<td>6.3.3 Users’ characteristics</td>
<td>105</td>
</tr>
<tr>
<td>6.3.4 Social communication</td>
<td>107</td>
</tr>
<tr>
<td>6.3.5 Management commitment</td>
<td>109</td>
</tr>
<tr>
<td>6.3.6 Implementation concerns</td>
<td>112</td>
</tr>
<tr>
<td>6.3.7 Cooperative Responsibility</td>
<td>124</td>
</tr>
<tr>
<td>Figure 6.11: Factors that influence on e-commerce security effectiveness from the customer and the organization perspectives</td>
<td>130</td>
</tr>
<tr>
<td>6.4 Relationships between categories and the core category</td>
<td>130</td>
</tr>
<tr>
<td>6.5 Conclusion</td>
<td>135</td>
</tr>
<tr>
<td>Chapter 7: Conclusions</td>
<td>136</td>
</tr>
<tr>
<td>7.1 Critical discussion and implications</td>
<td>136</td>
</tr>
<tr>
<td>7.2 Summary of Jordan Context</td>
<td>145</td>
</tr>
<tr>
<td>7.3 Research Findings and Literature Review</td>
<td>147</td>
</tr>
<tr>
<td>7.4 Research Contributions</td>
<td>150</td>
</tr>
<tr>
<td>7.5 Future Research</td>
<td>153</td>
</tr>
<tr>
<td>7.6 Research Evaluation</td>
<td>155</td>
</tr>
<tr>
<td>7.7 Limitations</td>
<td>156</td>
</tr>
</tbody>
</table>
Appendices .................................................................................................................................. 168
Appendix A: Example of transcribed interview with a customer in English and Arabic version, and extracted codes and concepts ........................................................................................... 168
Appendix B: Ethical Form ...................................................................................................... 172
Appendix C: Formal Letters ................................................................................................... 174
Appendix D: Samples of email correspondence with the participating companies ................. 176
Appendix E: Published Papers ................................................................................................ 183
Appendix F: Confirmation of identical translation .................................................................... 214
Appendix G: Description of organisations where data was collected from ................................. 215
List of Figures and Tables

Figures
Figure 2.1 Process of online credit card payment system with the involved participants
Figure 2.2 Security requirements in e-commerce
Figure 2.3 Holistic security management framework applied to electronic commerce
Figure 2.4 Security engineering lifecycle for e-commerce.
Figure 2.5 Framework for analysing e-commerce security
Figure 2.6 Dimensions of the framework for analysis of security in e-commerce
Figure 2.7 Initial Proposed Research Model showing the factors influencing the effectiveness of e-commerce security
Figure 4.1 Research design: Case study-Grounded theory Methodology
Figure 6.1 User characteristics category influences on e-commerce security effectiveness
Figure 6.2 Tangible and intangible categories that influence on e-commerce security effectiveness
Figure 6.3 The psychological aspect of security category influences on e-commerce security effectiveness
Figure 6.4 Cooperative responsibility category with the involved entities influences on e-commerce security effectiveness
Figure 6.5 Factors that influence on e-commerce security effectiveness from the customer perspective
Figure 6.6 The psychological aspect of security category that influences on e-commerce security effectiveness
Figure 6.7 User characteristics category influences on e-commerce security effectiveness
Figure 6.8 Social communication category influences on e-commerce security effectiveness
Figure 6.9 Management commitment category influences on e-commerce security effectiveness
Figure 6.10 Implementation concerns category that influence on e-commerce security effectiveness
Figure 6.11 Cooperative responsibility category with the involved entities influence on e-commerce security effectiveness
Figure 6.12 Factors that influence on e-commerce security effectiveness from the organization perspective
Figure 6.13 Interrelationships between categories that influence on e-commerce security effectiveness from the customer and the organization perspectives
Figure 6.14: Research model of the effectiveness of e-commerce security from customer and organisation perspectives, resulting from grounded theory analysis
Tables

Table 2.1 Summary of factors affecting customers’ perceptions of e-commerce security
Table 2.2 Analytical Framework
Table 2.3 Previous contributions considering the relation between the participant’s perspective and the research type/method
Table 3.1 Comparison between IS research paradigms
Table 3.2 Main characteristics of case study
Table 4.1 Grounded Theory Variants
Table 5.1 Case Study Protocol
Table 6.1 Tangible and intangible security features of e-commerce websites from customer’s perspective
Chapter 1: Introduction

1.1 Introduction

The development and advance of Internet technology has contributed to changing individual lives and the world. It can be seen that many things benefit from Internet facilities, such as e-commerce, e-business, e-government, e-banking, and e-learning. Although the importance and the advantages of this revolution are acknowledged by organisations and individuals, Internet applications still require a sufficient level of security and privacy (in perception and practice) to succeed and to be increasingly adopted.

Many technical solutions have been found and are being used to provide hard security in e-commerce applications. However, the Information System (IS) viewpoint concentrates on the people together with the systems that they interact and communicate with.

"Information systems are human-related systems: humans design and develop the hardware and software; humans operate the computer systems controlling the organisation’s corporate information database, and humans use the computers and information in their areas of work" (James, 1996, p. 11).

Therefore, an aspect of IS security additional to the technical, which relates to humans and their environment, is involved. The belief that security is the concern only of technical specialists, and the used security mechanisms and tools, have waned, because considerations of security require the contribution of technical and non-technical alike, since many security breaches arise not only from the security technology itself but also from (unconscious) human mistakes. For example, the social engineering approach where malicious people use tricks to exploit user unawareness of security and obtain private information is not a technical but a social problem.

Previously, researchers and academics have concentrated their work principally on technical issues of security, such as cryptography, algorithms and access control mechanisms in networks which are involved in information security. Although these are important, technological security alone cannot lead to an adequate solution. Security does not work effectively unless the people
concerned decide to make it work. Furthermore, a successful implementation of security solutions in e-commerce websites without customers being aware of it is meaningless. Thus, more recent researchers have realised that security is not just a technical issue, but rather that it involves managerial, organisational and human dimensions in order to be more effective (Von Solms, 1999; Von Solms, 2001; Eloff and Eloff, 2003; Bjorck, 2004; Tsujii, 2004; Ho & Chang, 2006; Shalhoub, 2006, Zuccato, 2007).

This thesis considers e-commerce security from two perspectives: the organisation (comprising IT and managerial personnel) and the customer. Because the people dimension is embedded in interactions with e-commerce applications, the nature of this research falls within IS research as it comprises both technological and organisational perspectives; therefore, as advised by Katsikas et al. (2005), the problem of e-commerce security should be addressed within an IS scope.

1.2 Information Security Surveys

Many surveys which have been conducted in the world into the problem of IT security reveal where improvements are needed regarding 1) the existence of security policies and/or procedures for implementing them, and 2) customer and organisation awareness of both technical and non-technical security issues. The remaining paragraphs in this section summarise the key aspects of these surveys.

The Global Security Survey, carried out by Deloitte in 2006, shows that internal security threats to an organisation continue to increase over previous years (employee misconduct 20%, internal financial fraud 19% of the threats) (www.deloitte.com). Another survey by InfoWorld (2006) of 430 qualified individuals responsible for their organisations shows that 42% of respondents reported that their organisation had no documented security policy. The responses considered (unintentional) employee error to be one of the top threats, besides others such as trojans, viruses, worms, spyware and spam. The respondents rated employees' underestimation of the importance of following a security policy as the most serious security challenge for their organisations (http://www.infoworld.com).
The Computer Crime and Security Survey was conducted by the Computer Security Institute (CSI) in 2006. Its results are based on the responses of 616 computer security practitioners in the US and show that virus attacks continue to be the source of the greatest financial losses. Unauthorised access continues to be the second greatest source of financial loss. The survey also shows that a majority of organisations view security awareness training as important (http://www.gocsi.com).

The 2006 Australian Computer Crime and Security Survey conducted by AusCERT in 389 public and private organisations showed that 60% of these organisations saw “the need to change users’ attitudes and behaviour regarding computer security practices” as the most common challenge for their organisation (http://www.auscert.org.au).

With regards to e-commerce security from a customer perspective, there are also surveys that confirm the problem of security. According to the Gartner survey of 5,000 online US adults in 2006, about $913 million was lost in e-commerce sales that year because of security concerns among online shoppers (http://www.gartner.com). This indicates that customers either do not perceive the required security or do not have enough knowledge of the security features that should be placed on the e-commerce website. This was confirmed by the Get Safe Online survey that was conducted through the UK’s first national Internet security awareness campaign in 2006 to investigate online behaviour and attitudes to Internet security. It showed that only 27% of respondents declared themselves very knowledgeable about PC security and confident about staying safe online (www.getsafeonline.org).

Within Arab countries, according to Aladwani (2003), Internet security was ranked the first concern for customers and business managers with respect to e-commerce usage. In Jordan, no specific survey has been completed with regard to security perceptions in e-commerce, but other related studies include that conducted by Alsmadi (2004) to investigate the attitude of 500 Jordanian customers toward online shopping. He found that the issue of security of online transactions was a major factor limiting their willingness to make greater use of online shopping.
1.3 Motivation

The motivations of this research are:

1. Many researchers state that security is a challenge and the main barrier to the successful implementation of e-commerce (Attaran and Vanlaar, 1999; Hawkins et al., 2000; Antón & Earp, 2000; Daskapan, 2001; Kesh et al., 2002; Labuschagne & Eloff, 2002; Jarupunpho & Mitchel, 2002; Albuquerque & Belchior, 2002; Katsikas et al., 2005). In particular, recent surveys, as discussed in Section 1.1, reveal that security is still the main concern for organisations and customers, and there is a need to explore the nature of this challenge and the current state of security perception from the perspectives of customers and organisations in respect of the use of e-commerce.

2. In the literature, and from the IS perspective, most security research relevant to e-commerce focuses either on the organisation (including technical implementation) or on the customer. Some of these studies identify the processes and factors required to implement a secure e-commerce application from the organisational perspective (Knorr & Rohrig, 2001; Lichtenstein & Swatman, 2001; Kesh et al., 2002; Ruppel et al., 2003; Hutchinson & Warren, 2003; Sengupta et al., 2005; Zuccato, 2007). Other research investigates customers' perception of security and risk awareness in e-commerce (Salisbury, 2001; Chellappa, 2002; Suh & Han, 2003; Kit & Jamieson, 2003; Milne et al., 2004; Yenisey & Salvendy, 2005; Singh, 2006). Little research has explored e-commerce security as a single phenomenon by considering the customer and the organisation jointly as the main participants in e-commerce. Such research would allow organisations to use certain security solutions that support customer's objectives and perceptions so as to reduce the gap between the technology being implemented by organisations and that being perceived by customers. Mistaken actions by the organisation could then be corrected to meet the customers' perceptions, as well as fostering a better understanding of the nature of Internet users. Furthermore, this would enable the researcher to highlight the differences and similarities between the two perspectives. There is no mention in the literature of the interrelationships between the factors and their relative impact on the effectiveness of e-commerce security. This research fills this gap by identifying and relating factors identified from both the customer's and the organisation's perspectives.
Most of the existing research that has been conducted in Jordan confirms the security concerns in e-commerce and Internet banking, but without exploring the issue in depth (Sahawneh, 2002; Alsmadi, 2004; Al-Sukkar, 2005; Titi, 2005; Al-Qirim, 2007). This makes Jordanian organisations and customers alike hesitant to participate in e-commerce, thus restricting the growth of e-commerce. Therefore, security in e-commerce is a vital area of research both globally and specifically in Jordan. Moreover, this research will be the first of its kind in Jordan to focus on e-commerce security from customer and organisational perspectives; a field in which there is a current lack of empirical research.

1.4 Objectives

The objectives of this research, based on the above considerations, are:

1. To extend the existing body of academic and theoretical knowledge regarding security considerations in e-commerce; by exploring the factors that influence the effectiveness of e-commerce security from both customer and organisational perspectives; and to show how they interrelate.

2. To provide practitioners, including IT managers and decision-makers, with a broad understanding by proposing a model which explains the connections among the relevant factors that affect e-commerce security in Jordan and which guides Jordanian IT managers in making effective e-commerce decisions, which ultimately facilitate the adoption of e-commerce.

1.5 Research Questions

The general research question is thus:

What are the factors and their interrelationships that influence the effectiveness of e-commerce security in Jordan?

This main research question can be usefully divided into three sub-questions:

1. What is the customer's view and perception of the security of e-commerce-website?

2. What is the organisational view of the managerial, technical and customer concerns regarding e-commerce security?
3. How can the organisational and customer views on e-commerce security be integrated into a coherent framework that provides guidance to decision makers?

1.6 Organisation of the Thesis

This thesis is divided into seven chapters. This first chapter has set out the scope and motivation of this research, referring to some significant gaps which have been found in the literature, highlighting some facts concerning information security and presenting the objectives which have led to the formulation of the specific research question and its associated sub-questions.

Chapter Two provides an introduction to e-commerce and information security, and presents the theoretical basis of this research; it discusses the existing e-commerce security models and frameworks, and the customer perception of security. It provides a framework of analysis for the prior literature that is relevant to e-commerce security from the IS perspective, which helps to identify some gaps that can be covered by future research. The last part of this chapter reviews the development of ICT and e-commerce in Jordan, as this will be the target context of the fieldwork of this research, and presents previous studies that have been carried out in Jordan, which provide evidence of a security challenge for the successful adoption of e-commerce.

Chapter Three focuses on the research methodology. It reviews the research paradigms in the IS field in general and in the IS security domain in particular. It provides an overview of different research methods that are used in IS research. This chapter also explains the case study research approach and gives a justification for adopting interpretive case study research as an appropriate method in this instance.

Chapter Four complements the previous chapter. It elaborates the grounded theory method, as defined by Strauss and Corbin (1990), as a tool of analysis for the qualitative data that is collected from the case studies. It also justifies the use of grounded theory in a manner compatible with the case study research method to form ultimately the research methodology that is adopted in this thesis.
Chapter Five sets out the context in which the data were collected. It presents the procedures for selection of the cases and the unit of analysis in this research, elaboration of the case study protocol and on the procedures that were followed before undertaking the fieldwork and during data collection.

Chapter Six provides an analysis of the data on customer and organisational perspectives. The findings are presented as categories which result from the application of grounded theory procedures, representing the factors that influence the effectiveness of e-commerce security. The combination of these factors and the interrelationships between them are also presented in the form of a model at the end of this chapter.

Chapter Seven provides a critical discussion and draws implications from the above findings, making comparisons between the research findings and the prior literature. This chapter concludes by highlighting the theoretical and practical contribution of the research and making suggestions for future research. It also provides an evaluation of the whole research process, and highlights the limitations of this research.
Chapter 2: Literature Review

This chapter presents an introduction to e-commerce and information security, and discusses the relevant literature on security models and frameworks in e-commerce. Such security models clarify how companies can follow a systematic process for building secure e-commerce applications, so that they are more oriented towards the organisation, or alternatively so that they can consider the role of technical experts who develop and implement secure e-commerce applications. This chapter also highlights customers' perceptions of security in e-commerce. It identifies and tabulates the factors that influence such perceptions, including customers' stances and beliefs. A review of the current academic literature on e-commerce security from an IS perspective allows the construction of a framework of analysis of earlier studies and an initial research model based on the survey of the literature.

The final part of this chapter provides background information on Jordan and outlines the development of Information and Communication Technology (ICT) and e-commerce in the country. This section also presents evidence from key research that has been carried out in Jordan to substantiate that security is a barrier to the adoption of e-commerce and e-banking.

2.1 Definition and overview of E-commerce

E-commerce, or electronic commerce, can be defined as a process of buying and selling products, and/or of transferring services and information, over the Internet (Turban et al., 2006). Choi et al. (2000) distinguish types of e-commerce based on the degree of digitization along three dimensions: product, process and delivery agent. For example, if a customer buys a film or software, downloads it directly to his/her computer and pays electronically, then this is called pure e-commerce. If one of these dimensions is operated physically, then this type of transaction is called partial e-commerce. Rowley (2000) and Rao and Metts (2003) proposed a stage model for e-commerce development. For example, Rowley (2000) states that the development of e-commerce applications passes through four stages:

1. The first stage is contact, where the website has a marketing function, promoting products and publishing information.
2. The second stage, interaction, is concerned with exchanging information, communicating
with customers and searching for information via the website.

3. The third stage, transaction, enables financial operations to take place through ordering, cataloguing and online payment systems.

4. The last stage, community, is where a two-way partnership between customer and organisation is established, allowing customers access to the organisation’s database.

It is important to attempt to clarify the relation of e-commerce to another similar term, ‘e-business’. Many authors state that e-commerce is a subset of e-business (Chaffey, 2004; Turban et al., 2006; Bidgoli, 2002; Rowley, 2002; Beynon-Davies, 2004), claiming for instance that the latter covers many business activities which are not included in e-commerce, such as servicing customers and collaborating with business partners (Turban et al., 2006; Rowley, 2002; Bidgoli, 2002) or processing a purchasing order (Chaffey, 2004). E-business involves integration across business activities and communication within the organisation (Rowley, 2002), as well as web advertising, supply-chain management, order management, sales force automation and electronic payment systems (Bidgoli, 2002).

In contrast, Schneider (2007) considers e-commerce to be broader than e-business. In support of this position, Carter (2002) states that some people use e-commerce to encompass e-business because e-commerce includes Business to Business (B2B) activities (see next section for a definition of this concept). Sengupta et al. (2005) use e-commerce in its broadest sense, stating that a good definition of e-commerce mentions the use of electronic data transmission to support business processes. Regardless of whether there is an acceptable resolution to the argument as to which is wider, or whether both concepts are similar, in this research the term ‘e-commerce’ will be used.

### 2.2 E-commerce categories

There are many categories of e-commerce. These are typically classified according to the nature of the transaction and the participating entities (Schneider, 2007). The three main categories that are distinguished are:

1. Business to Customer (B2C), where a business sells a product or service to an individual person.
2. Business to Business (B2B), where all participants are business organisations.

3. Customer to Customer (C2C), where one individual customer transacts with others.

Auction websites (e.g. ebay.com) are one of the most well-known types in this category.

Another category sometimes identified is Customer to Business (C2B), which represents customers telling companies what they want individually (Wong et al., 2005), or where a customer sells products to a company. Some authors mention even more categories, such as Business to Employee (B2E), Government to Customer (G2C) and Government to Business (G2B) (Turban et al., 2006; Schneider, 2007). In respect of security, it can be said that it is involved in all e-commerce categories, but it is important to take into consideration that B2B activities are much riskier than B2C or C2C, because the size of payments between businesses is larger than other categories, so tight security is required (Bernardi, 2002). Furnell (2005) states, although the largest volume of transactions occur in B2B, the organizations engaging in B2B transactions can reasonably be expected to have some level of competent IT and security enforcement. This is not guaranteed when dealing with customer (i.e. end user) in B2C scenario, so he considers B2C e-commerce is riskier. This research will specifically address Business-to-Customer (B2C) and Customer-to-Customer (C2C) e-commerce websites.

2.3 Participants in E-commerce

According to Hassler (2001), if electronic payment is involved in e-commerce, then four types of participant are required: customers, merchant (i.e. organisations), and issuer and acquirer banks. The issuer bank is a financial institution that issues a credit card to a customer and responds to an online payment request from the acquirer bank (i.e. merchant bank). Figure 2.1 presents the basic electronic payment transaction process with the involved participants.

Typically, a customer orders a product online from a merchant’s website and fills in the “checkout” page with credit card information through a secure connection. The merchant receives the customer’s order information and checks the authorization and authentication of the credit card information by sending it to the clearinghouse (i.e. this intermediary is an electronic payment service provider linked to the Master Card or Visa network) which verifies account and balance with the issuer bank to confirm the authenticity of the customer. If it is accepted, then
the transaction proceeds and the amount is deducted from the customer’s credit card and transferred from the issuer’s bank account to be deposited into the merchant’s bank account (acquirer bank).

![Diagram of online credit card payment system with involved participants](image)

Figure 2.1: Process of online credit card payment system with the involved participants


### 2.4 Benefits of and barriers to E-commerce

“All advantages of electronic commerce for business can be summarised in one statement: electronic commerce can increase sales and decrease costs” (Chaffey, 2004, p.17). Turban et al. (2006) state that the benefits of e-commerce impact on the organisation, the individual customer and society.

Benefits to the organisation include the global reach from any part of the world; e-commerce expands the organisation’s market and consequently increases its sales, reducing the cost of creating and storing paper-based information, opening 24 hours a day, 7 days a week, therefore attracting more potential customers. It also improves the relationship with customers and allows each one to be dealt with in a personalised way. This leads to better customer satisfaction, and as a result the organisation may retain the customer for longer.

The benefits of e-commerce to the customer include allowing customers to shop at anytime and from any location. E-commerce also provides customers with many choices of sources and
prices, and enables them to make comparisons between companies and subsequently to select the best product for their particular needs at the best price. Furthermore, immediate delivery in the case of digitized products (e.g. music, software and books) and the availability of information when it is needed are also significant benefits.

The benefits to society include enabling people in poorer countries to enjoy services and products that were not available previously. In addition, e-commerce enables people to work and shop from their homes, which serves to reduce traffic and air pollution.

One feature of e-commerce is that of being a virtual environment. This can sometimes limit the use of the Internet for buying and selling tangible products such as jewellery (Schneider, 2007), where the customer likes to touch products before purchasing. In addition, there are limitations concerning legal issues in respect of regulations that organise the online transactions, and questions of trust, privacy and security of the electronic payment and personal data (Sengupta et al., 2005; Turban, 2006; Schneider, 2007). Many researchers state that security is the primary challenge and concern for the successful implementation of e-commerce (Attaran and Vanlaar, 1999; Hawkins et al., 2000; Annie & Earp, 2000; Daskapan, 2001; Kesh et al., 2002; Labuschagne & Eloff, 2002; Jarupunpho & Mitchel, 2002; Albuquerque & Belchior, 2002; Katsikas et al., 2005).

2.5 Definition of IS Security

Security in IS has changed significantly over the years. It began in the 1960s with a concentration on cryptography algorithms and the security of operating systems. During the mid 1990s, as advanced computer communication was developed, human factors started to be addressed. Where the use of Internet capabilities supporting business processes emerged, then attention turned towards the security of e-business (Trcek, 2004).

According to Udo (2001), security is defined as the protection of data against accidental or intentional disclosure to unauthorised persons or against unauthorized modification or destruction. This definition focuses on data security. Other broader definitions (Pipkin, 2000; Nixon et al., 2005) state that security means reducing the risk that is likely to occur in the
resources of an organisation (e.g. people, information, property, and infrastructure). Security can be enforced by evaluating the risk of bad things happening in a certain environment or situation, and developing safeguards and countermeasures against these risks.

Security has been seen as a process, not as a product (Centeno, 2002; Schneider, 2000). For example, a house whose door has good locks but where the windows are open and the keys are given to neighbours is very vulnerable. Who has permission to open the door and hold the keys: all family members, or only the father and mother? When do they open the door and when do they close it? The aim of this scenario is to show that security is not just the presence of locking of the door by using robust hardware and software, but that there is a human dimension which must be considered, as well as the policies and procedures that are required to make the house remains secure. In an IS context, similarly, security involves both managerial and technical measures to protect the organisational assets (information, hardware, software) against unauthorised access, modification, use or disclosure (Hong et al., 2003; Shalhoub, 2006).

Katsikas et al. (2005, p.7) cite the comprehensive security definition of Kiountouzis (2004), namely that it is “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 encapsulates two main aspects which are needed for understanding the nature of security in e-commerce. The first is the perception and awareness of security from the participant’s viewpoint, which is subjective to the individual, defined by Salisbury (2001, p.2) as concerning “the extent to which one believes that the Web is secure for transmitting sensitive information”, such as credit card or social security number. The second aspect is the policies, measures and techniques that should be implemented by the organisation to protect its e-commerce websites.

2.6 Information and E-commerce Security Requirements

The terms ‘security requirements’ and ‘security objectives’ are used interchangeably (Lamsal, 2001). According to ISO IEC 1799 (2000) and Gerber & Von Solms (2001), there are three basic information security requirements: confidentiality, integrity and availability, required in the
context of IS. An e-commerce system can be considered as a kind of IS so these three requirements are required for e-commerce as well. However, e-commerce systems involve the customer's engagement directly. Therefore, the scope of security should be expanded to comprise the customer's perception, from one hand. Furthermore, e-commerce system requires the Internet as a main medium to accomplish its purpose; buying and selling online, where it can be said that any machine connected to the Internet is potentially vulnerable. This is not the case for all types of IS (i.e. not Internet-based IS) that are installed within the organization, and consequently additional security requirements are entailed for an e-commerce environment as presented in the following paragraphs.

Many authors have listed additional requirements for a secure e-commerce environment, such as non-repudiation, authentication (Kesh et al., 2002; Ratnasingham, 1998; Jarupunphol & Mitchell, 2003; Sengupta et al., 2005; Shih, 2002; Gardiner, 2003; Turban et al., 2006) and authorisation (Ratnasingham, 1998; Sengupta et al., 2005; Shih, 2002; Turban et al., 2006). Some authors have used the terms 'privacy' and 'confidentiality' to have identical meaning (Kesh et al., 2002; Turban, 2006), while 'access control' is same as authorisation (Kesh et al., 2002). Turban et al. (2006) consider auditing as one of the major security requirements. Each of these requirements is explained below in more detail.

Confidentiality (privacy) means that sensitive or private information should be protected from unauthorised disclosure, so that only legitimate users can access it (Kesh et al., 2002; Turban et al., 2006). Loss of confidentiality can affect a customer's information, such as his/her name, address, account number, credit card number, e-mail address and purchasing history, or a company's information, such as price sheets, new product specifications or corporate investment strategies (Pipkin, 2000); any of these can have serious consequences for customers and/or companies. On the company's side, the disclosure of sensitive information may cause the business to lose sales and market position (Pipkin, 2000), while on the customer's side, their trust in organisations to whom they have disclosed their information will be curtailed or lost if their private information is made known freely. In addition, a company can suffer indirect damage if legal action is taken by those individuals who have lost their privacy (Pipkin, 2000).
**Integrity** of information means ensuring that data that has been transmitted electronically is not altered (Sengupta et al., 2005; Turban et al., 2006) or destroyed during transmission or storage, either accidentally (e.g. via transmission errors) or with malicious intent by a hacker. Integrity ensures that only authorised users can make changes to such information (Kesh et al., 2005). Companies need to ensure that their information exchanged over the Internet has not been modified. These modifications could take the form of the creation or deletion of documents, or the changing of web contents (Kesh et al., 2005). This modification leads to risk and financial damage or loss, because inappropriate decisions are made based on faulty information, besides providing misinformation for the customers on the website (Pipkin, 2000), and as a result company reputation can be significantly damaged.

**Availability** ensures that the required information and services are available when they are needed. For an e-commerce website this means that the customer order systems are available when the customer wants them (Kesh et al., 2005). For example, if a customer is willing to execute a stock trade transaction via an online service, then that service should be available in real time (Turban et al., 2006). According to Pipkin (2000), availability is considered a very important attribute for any business that depends on instant information, such as an airline schedule or an online inventory system, where the inability to access information to make decisions immediately when needed affects profits.

**Authentication** is “the process by which one entity verifies that another entity is who he, she, or it claims to be” (Turban, 2006, p.462). In e-commerce websites, the company needs to make sure that the person using the credit card is the owner of the card and in the same way the customer needs to make sure of the identity of the company. Without appropriate authentication, it is impossible to know who actually placed an order and whether the order placed is real or not (Kesh et al., 2005). Authentication is therefore the basis of trust (Pipkin, 2000) and when the identity of one party is unknown to the other, then trust will be reduced.

**Non-repudiation** ensures that the sender cannot deny sending a particular message and similarly the receiver cannot deny receiving a message (Kesh et al., 2005). For example, a customer may deny that an order was placed or that goods were delivered, or the company may deny receiving
an order or that a payment was made.

**Authorisation** or access control ensures that legitimate access to systems, resources or business functions can be gained only by authorised users, while those without valid access are excluded (Ratnasingham, 1998; Kesh et al., 2005). This includes physical access and logical access to resources where the former occurs by entering a building or accessing computers and servers, while the latter means obtaining permission to access or log into the systems (Kesh et al., 2005). It is important to note that even when system resources are accessed by an authorized user, other security requirements may be broken (Kesh et al., 2005); for example, a person who has privileged access to a system can seriously interfere with the integrity of information.

**Auditing** is, according to Turban et al. (2006), a process of collecting information about resources (e.g. database queries) that have been accessed using particular privileges or performing another security action like modification of database records (i.e. violation of integrity). This information is kept in log files, which enable IT personnel to identify the user or the program that performed a certain action.

Each of the main participants in e-commerce (i.e. customers and organisations) has different security concerns and requirements (Knorr & Röhrig, 2000; Shih, 2002). Customers are concerned with privacy/confidentiality and the integrity of transmitted information (Shih, 2002), while organisations (merchants) may be interested in the identification and authentication of customers, non-reputation, the availability of the services (Knorr & Röhrig, 2000; Shih, 2002), the integrity of information on the website and its own approach for respecting its customer’s privacy (Knorr & Röhrig, 2000).

Scambray (2000) shows the place of each security requirement on the customer’s web browser, the merchant’s server and through transmission, as depicted in Figure 2.2.
In essence, although as mentioned above security requirements are involved for both customers and organisations, it should be taken into consideration that the customer is the weaker party. This is because s/he has to pay before receiving the product or service, has to release his/her private information (e.g. credit card number) and cannot touch or see the product, all of which may make a person hesitant to purchase online. Nevertheless, if it is assumed that the major risks come from outside those two parties, such as from hackers and attackers, then customers and organisations are equally vulnerable.

The relation between security and e-commerce is clarified by Zucatto (2002), who states that security can be seen as a business enabler, where the acceptance of the e-commerce is dependent on its security functionality. In other words, customers decide to sell or buy products and services because they expect security to be provided; thus the perception of sufficient security increases the usability of e-commerce. The reverse is also true, in that insufficient security perception and implementation reduces the usability of e-commerce websites. Hence, security is seen as a business requirement (Pipkin, 2000), because companies need adequate security to protect their assets and resources.

To summarise this part of the literature review, the definition of e-commerce has been clarified, and its main categories and participants, and there has been an examination of the benefits of e-commerce, its barriers. Information security has also been defined and its requirements explained from the perspectives of customers and organisations.
2.7 Security Models in E-commerce

This section discusses the existing models and frameworks in e-commerce from an organisational perspective. These primarily guide organisations in their development and evaluation of secure e-commerce applications.

Zuccato (2007) has developed a holistic framework for information security management which he claims can be applied to e-commerce. The meaning of ‘holistic’ here is that each activity within this framework takes into account three dimensions: business, technology and society.

Zuccato (2007) characterises the framework as process oriented, with five core processes/workflow and two support processes/workflows, as shown in Figure 2.3. It represents the first refinement of each workflow, where under each one there are further sub-workflows. The five core processes are: 1) business modelling, where the organisation defines how the business model should be enhanced by security and which security functions are expected to generate business benefit; 2) project planning, which aims to develop plans of how to incorporate security into the operative business; 3) security analysis and design; 4) implementation and 5) maintenance. He provided under each process detailed activities which show the position of security in the organisation and during the e-commerce development process. The framework emphasises direct feedback between the activities, with iterative phases based on a system lifecycle model; it is people-centric, since people are considered in their roles as stakeholders, users, developers and decision makers.

The two support processes/workflows are those of business foundation and of humans and organisation. The objective of the business foundation workflow is to motivate and control the economic viability of the security investment, by integrating and connecting the security management process with the organisation’s objectives and overall management process. As for ‘humans and organisation’, this component of the holistic framework concerns the educational aspects of security with the aim of increasing awareness of security and building security literacy among individuals within the organisation, while also providing the motivation for security. This component includes other organisational activities such as human resource management, third-party management, creating a security culture, and top management support.
Within this framework, the environments as stated by Zuccato (2007) are significant because they contain constraints that influence the system and should be taken into account during the activities of management. As shown in Figure 2.3, the framework addresses two aspects of the environment, the *societal environment* being the top-level environment under which the whole system runs and is managed. *Societal environment* affects system behaviour by providing constraints and high-level requirements; it is the source of moral obligations and customer expectations. The *business environment* (i.e. the organisation) is the environment in which the security management has to be implemented. It has demands and constraints that guide the security management activities; it may also be considered as comprising the organisation’s culture and behaviour.
The component of privacy, which is considered significant in this framework, has according to Zuccato (2007) a strong relation to security; in addition, privacy can be a business enabler. In the holistic framework, Zuccato (2007) proposed to conduct privacy activities in parallel to the security workflows of business modelling, planning and analysis & design. The holistic framework also comprises standards for information security management such as ISO 17799 (information security standard includes guidelines, principles and practises for initiating, implementing, maintaining, and improving information security management in an organization), legislation, and ethics elements.

Sengupta et al. (2005) state that security in e-commerce is required to operate as a continual process rather than a one off product. This process approach is necessary to respond to any changes in business goals and technology development. They describe this process as a life-cycle, comprising security requirement specifications, risk analysis, security policy specifications, security infrastructure specifications, security infrastructure implementation, and security testing and requirements validation. Figure 2.4 shows the life cycle model, whose phases are examined in detail below.

1. **Security requirement specification and risk analysis.** In this phase, information about an organisation’s assets that need to be protected is collected, the threat perception is assessed for those assets, account is taken of the services requiring access to the assets and of the access control mechanism required for the services, and the associated access control polices are considered.

2. **Security policy specification.** This phase uses the “security requirement specifications” and “risk analysis reports” as input for formulating a set of e-commerce security policies. A security policy is a written document which defines the physical and IT assets of organisation, and how they can be protected and by whom. A security policy may include issues such as what kinds of information exist within the organisation and which have to be encrypted before being transmitted, and who has access to the organisation’s servers.

3. **Security infrastructure specification-** this phase analyses the “security requirement specifications” and the “security policy specification” from the previous phase to make a list of security tools that are needed to protect the assets. Security tools are technology
(i.e. hardware and software) used to secure the e-commerce such as a firewall, digital certificate and SSL.

4 **Security infrastructure implementation.** The organisation, in this phase, implements, deploys and configures the selected security tools and applications at the system level. The security infrastructure involves also implementing the security policy and managing the behaviour of human resources and their roles, besides the technology. For example, it determines who checks the written logs.

5 **Security testing.** In this phase, a set of tests are carried out to check the effectiveness of the security infrastructure and the functionality of the access control mechanisms.

6 **Requirement validation.** In this phase, analyses and evaluations are made to identify to what extent the security requirements of the e-commerce organisation are met by the corresponding security policy and the implemented security infrastructures. Changes in the business goal, operational environment or advanced technology may lead to an updated set of security requirements and then a fresh iteration of the "security engineering life cycle" will be undertaken.

![Security engineering life cycle for e-commerce.](image)

Figure 2.4: Security engineering life cycle for e-commerce.

Source: Adapted from Sengupta et al., 2005
Kesh et al. (2002) have also developed a framework for analyzing e-commerce security. The first step, as shown in Figure 2.5, is to evaluate the organisation's security needs. The second step is the analysis of the threats that can be faced by e-commerce. Once certain threats are identified, the organisation develops a list of technologies or solutions to be used. In the next step, organisations will select tools that support the chosen technology (e.g. SQL server tool supports encryption/SSL technology). In some cases the tools may include technology that has already been used by another tool. For example, if an organisation already uses Oracle-based applications, it needs to know the security technologies that Oracle supports in order to identify additional tools to be used to support security technologies that Oracle does not support. Another example is related to encryption: some tools support the encryption of data at different levels. For instance, Java supports encryption in the applications development platform layer, while Cisco routers do the same in the network infrastructure layer. Multiple levels of encryption will slow down the system but at the same time provide more protection. It is the role of a security administrator to decide which features should be selected, based on the level of security, time and cost. Finally, decisions are made by the organisation about the security architecture which comprises the technologies, the tools and their features.

![Figure 2.5: Framework for analysing e-commerce security](Image)

Source: Kesh et al., 2002

Hutchinson and Warren (2003) suggest a framework for Internet banking security. It is derived
from one for e-commerce security and consists of six steps:

1. List all the security requirements for Internet banking environment in general;
2. Identify all participants and stakeholders involved in the Internet banking process;
3. Break down transactions into different autonomous actions;
4. Map these identified actions on to the participants involved, which serves as a model for the Internet banking environment;
5. Use the information obtained in step 4 to determine the security requirements for a secure Internet banking environment;
6. Use these security requirements to develop the security architecture, comprising suitable security procedures, mechanisms and policies.

Knorr and Rohrig (2001) propose a three-dimensional framework for the analysis of security requirements of business processes in e-commerce. The main dimensions of the framework, as shown on Figure 2.6, are security objectives (confidentiality, integrity, availability and accountability) and the phases of the business process (information, negotiation, payment and delivery) and the parties that are involved in this process (customer, organisation). This framework enables the assessment of the security needs of each party for each business process by providing suitable mechanisms to support these needs. For example, at the payment phase of the business process an SET protocol can be used to support the integrity and provide authentication of both the customer and the organisation. Knorr and Rohrig (2001) also indicate that the level of security needs is variable for each party and for each business process. For instance, during the negotiation phase, where a contract is made between the parties, the customer has to reveal his personal information, which will make him more sensitive about confidentiality. Knorr and Rohrig (2001) pointed out that for the merchant, the confidentiality of the customer's data will be important as it is required by regulations (e.g. privacy laws).
Otuteye (2003) proposes a systematic approach to e-business information security. This approach comprises six stages for security management in e-business:

1. Develop a corporate risk consciousness and risk management culture.
2. Perform a thorough risk assessment of the whole business. Identify and rank risks based on threats, vulnerabilities, cost and countermeasures.
5. Follow systematic risk assessment and risk management procedures to determine the level of risk after implementing the best practices on each component. Insure residual risk of low probability but high cost events and manage the rest.
6. Monitor and audit diffusion of risk management culture, policy implementation and enforcement, and revise as needed.
Lichtenstein and Swatman (2001) identify the factors that influence the constructing of an effective e-business security management and policy. They are Internet risks, organisational, administrative, legal, societal and technical standards, and human factors.

The literature on information security suggests that top management support is an important factor for the effectiveness of information security in organisations. Kankanhalli et al. (2003) and Ho and Chang (2006) identify a set of organisational factors governing the effectiveness of implementing IS security, such as organisation size, top management support, the IT competence of business managers and industry type (for example, financial organisations have greater concerns for information security).

2.8 Customer’s security perceptions

As discussed in Section 2.7, several existing security models and frameworks clarify how companies can follow a systematic process for the building and analysis of secure e-commerce applications. These models and frameworks are oriented more towards the organisation and can be considered the particular domain of technical and expert people who develop and implement secure e-commerce applications. This section looks at relevant literature and discusses factors identified there as having an influence on customers’ perceptions of security. Table 2.1 summarises these factors.

From a customer perspective, the perceived security of an e-commerce transaction can be defined as “the subjective probability with which consumers believe that their personal information (private and monetary) will not be viewed, stored, and manipulated during transit and storage by inappropriate parties in a manner consistent with their confident expectations” (Chellappa, 2001, p.16). Customers’ perception of security is necessary to successful e-commerce because even if a certain company uses the best technical solutions to provide full security, without the perception or awareness on the part of the potential customer that its website is secure, these technical solutions can mean nothing.
Sharma and Yurcik (2004) identify a set of factors that influence the customers’ perception of the security of an e-tax filing website. They state that “if people are able to perceive the websites as secured and trustworthy they will be able to believe in the security and privacy measures available on these websites” (p.5). This relates to the beliefs and attitudes toward certain websites. Users’ knowledge and experience also help to enhance their perception of security. Milne (2004) states that an educational initiatives by businesses and the public sector help customers to recognise the risks of online identity theft, which leads to more awareness of security. Sharma and Yurcik (2004) identify several factors, such as ease of use, which refers to the feeling of security experienced by the user and the feeling of control over the interactive system, such as submitting data when filing a tax return, which makes the user feel confident. A security and privacy policy on a website will also increase the user’s perception of its security and credibility by providing descriptions of the security technologies employed. Sharma and Yurcik (2004) state that a security policy increases users’ perceptions of security even though

Table 2.1: Factors affecting customers’ perceptions of e-commerce security

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Attitude and motivation toward security</td>
</tr>
<tr>
<td>2</td>
<td>User’s knowledge and experience, Education</td>
</tr>
<tr>
<td></td>
<td>Usability: (ease of use)Presentation/interface/layout</td>
</tr>
<tr>
<td>3</td>
<td>Privacy and security statements of policy</td>
</tr>
<tr>
<td>4</td>
<td>Presence of SSL encryption by small lock, and web browser supporting 128-bit encryption</td>
</tr>
<tr>
<td>5</td>
<td>Support authentication/logon PIN/strong password</td>
</tr>
<tr>
<td>6</td>
<td>Third party security seal e.g. VeriSign</td>
</tr>
<tr>
<td>7</td>
<td>Third party privacy seal e.g. TRUSTe</td>
</tr>
<tr>
<td>8</td>
<td>Presence of demo and FAQs</td>
</tr>
<tr>
<td>9</td>
<td>Presence of physical address, company name, phone no.</td>
</tr>
<tr>
<td>10</td>
<td>Download time/timeout though submitting form</td>
</tr>
<tr>
<td>11</td>
<td>Digital certificates</td>
</tr>
<tr>
<td>12</td>
<td>Funding and company security budget</td>
</tr>
<tr>
<td>13</td>
<td>Top management support</td>
</tr>
<tr>
<td>14</td>
<td>Updated security technology</td>
</tr>
<tr>
<td>15</td>
<td>Dynamic policy statement</td>
</tr>
<tr>
<td>16</td>
<td>Electronic receipt and acknowledgement</td>
</tr>
</tbody>
</table>
they may not be able to understand its contents. Using authentication mechanisms (e.g. PIN numbers), the Secure Socket Layer (SSL) protocol with 128-bit data encryption, and third-party trust symbols like VeriSign also increase the perception by customers that a website is secure. However, Sharma and Yurcik (2004) state that there is misuse of third-party symbols on some websites, where some of the signs have been found to have no real links, but are just graphic images. According to them, another factor which could affect the perception of security is the use of demonstrations (demos) and Frequently Asked Questions (FAQs). Demos help users to create a mental navigation map and enable them to keep mindful track of the links. FAQs are also useful for website users, especially first-time users who have queries about the system and how exactly it works. Finally, the statement of a physical address on the website increases the feeling that it is secure and credible.

Turner et al. (2000) investigated factors affecting the e-commerce security perceptions of expert and normal users. From an end user’s perspective, they found that there were different attitudes toward the security of an e-commerce website. Some participants were concerned with security on the Internet and were aware of security-related problems that might occur, while some saw security as unimportant and assumed that it would be provided sufficiently by the website operators. Other participants were concerned about security, but only when money was involved. This highlights an important factor, which is the beliefs of customers about security, each customer having a different attitude, which could also refer to their motivation and their interpretation of security. For example, a customer may have heard that online banking is insecure and risky. On the other hand, this customer may hear that his friend performs all of his bank transactions online from his home in complete security, while he himself negotiates heavy road traffic to go to the bank, where he sometimes has to queue for a long time. Therefore, he decides to learn about the risks affecting online banks and what security technology and practices he needs to know to overcome these risks in order to engage in e-commerce. Thus, it can be said that motivation leads to changes in attitude. Siponen (2000) states that attitude and motivation are important factors for security perception and culture within organisations. In this regard, he distinguishes between motivation and attitude: motivation tends to be dynamic in nature (lasting from minutes to weeks), while attitude is a more static set of beliefs and assumptions in the mind (lasting from months to years). It can be said, in summary, that attitude and motivation are vital factors influencing customers’ perceptions of security in regard to e-commerce.
Another set of factors, which were mentioned by users in a study by Turner et al. (2000), were the long page download times combined with other problems with the site, such as page timeouts when submitting forms, or websites frequently going down. These could indicate that a site has been poorly implemented and may therefore not be secure. Use of a symbol on a page, like those of TRUSTe and VeriSign, indicates that customers' information is protected. Other factors affecting customers' perceptions of security include SSL and data encryption (as indicated by <https> in the browser address), verification of digital certificates, the browser padlock symbol in the corner of the page, and websites which support the use of robust passwords. Expert respondents stated that site presentation issues—including look and feel, the use of graphical symbols, the presentation of available information on site layout and navigation, and statements of company security policy—were not directly related to perceptions of security, but were considered as indications of a company's professionalism and commitment to customer service.

Yenisey et al. (2005) identify many factors affecting e-commerce security perceptions among Turkish people. The website's funding and the budget allocated to security can be considered as directly influencing perceived security. Increased funding would improve the overall secure feeling of users while shopping online. The commitment of the website's top management to security is an important factor, as part of increasing customer awareness of security-related issues in e-commerce. As mentioned by Yenisey et al. (2005), it is important for customers to know that security is an issue being taken seriously by the website at a management level. They suggest that it can be presented as a policy statement by the company at the entrance to the website, with a message saying “this company is entirely committed at a top management level to providing full security for its customers by applying security procedures”.

E-commerce websites often give prominence to their login procedures and to name and password-based authentication, to make the user aware of their concern for customer protection (Yenisey et al., 2005).

The question of whether the website is kept up-to-date with product standards to the extent of
applying a constant updating of the security systems will affect the perceived security of the users. This updated state of security features can be presented to users via messages including the version details of the security software and hardware being used on the website, also indicating that they are the latest versions (Yenisey et al., 2005). The encryption method of a website in e-commerce can be presented to users in a message during transactions. Yenisey et al. (2005) note that e-commerce companies do not currently allow users to conduct transactions with web browsers only capable of less than 128-bit encryption. The user’s web browser information is checked by the website; therefore, presenting their own browser information to users is believed to be a perceived security enabling factor (Yenisey et al., 2005).

A study by Gauzente (2004) suggests that e-commerce websites should implement privacy and security measures and present them in a policy statement or chart in order to increase the perception of security. They also suggest that in order to reduce consumers’ reluctance to provide sensitive information, web merchants should adapt their privacy and security statements according to consumers’ browsing intentions. For example, when consumers ask for information, a dynamic link should be generated to a page where a statement underlines areas of policy that are of prime importance at this stage of the relationship (that is, “information sharing”, “information transmission security” and “information storage horizon”). Likewise, when a consumer places an order, another link should be generated whereby the overall policy is presented with an emphasis on “access to information” and “use of information”.

Centeno (2003) indicates measures that could enhance consumer protection in e-commerce applications, some of which are: checking the seller’s reputation (in auctions); checking the company’s security policies and the tools used, in particular for personal data protection; checking privacy policy and how personal details may be used; keeping a trace (via e-mail) of order screens, terms and conditions, and any communication with the merchant; and verifying the merchant’s identity and company information, such as its name, physical address and telephone number.

Singh (2006) reports empirical findings that the most effective way to increase the perception of
Internet banking security is to increase ease of use, to improve the convenience and usefulness of online banking and to offer customers a more personalised experience of online transactions by giving them greater control of their transactions and information.

There are also studies providing evidence that a perception of security increases trust in e-commerce websites and consequently increases the intention to transact online (Chellappa, 2002; Salisbury et al., 2001; Suh and Han, 2003; Pennanen et al., 2006; Connolly & Bannister, 2007).

2.9 Analysis of Existing Frameworks.

The analysis of the existing literature on e-commerce security, from which studies conducted between 2000 and 2007 which were also related to the IS field were selected, is based on four criteria: the participant’s involvement and perspective, the contribution of the research, the research paradigm/method, and the type of research. These criteria are now considered in turn.

1 **Participant’s Perspective**: The main participants in e-commerce are the customer and the organisation (i.e. merchant). Most existing research focuses on the customer or the organisation, with very few combining both as holistic concept to be integrated.

2 **The contribution of the research**: The contribution of previous studies of e-commerce security can be classified according to the principal participants (i.e. customer or the organisation) they consider. The first contribution is from the organisation’s perspective. Most of the existing research concerning this perspective identifies systematic processes and factors that are required to implement secure e-commerce applications. A systematic e-commerce security process is similar to the IS development processes like system development life cycle (SDLC), but considers the security functions at all stages of development—requirements analysis, design, implementation and testing—by including the supportive tools and technologies, and providing a framework for assessing security requirements in e-commerce. The second contribution is from the customer’s perspective. This focuses on exploring the customer’s perceptions and beliefs concerning security controls and features and on identifying the factors influencing these perceptions. The contribution of this perspective also provides evidence of the impact of the perception of
security on trust in—and consequently engaged with—e-commerce applications

3 Research method: IS research methodologies are very important, being of significant concern in studying IS phenomena, so this criterion, which distinguishes different schools of thought concerning the IS phenomenon, was considered in the analytic framework. Orlikowski and Baroudi (1991) and Klein and Myers (1999) distinguish three paradigms of IS research: positivist, interpretive and critical (see chapter 3 for detailed definition of these research paradigms). Questionnaire/survey and experiment are examples of quantitative research methods, which are typically belonging to the positivist paradigm. Action research, case study research, ethnography and grounded theory are all examples of qualitative research methods, which are always belonging to the interpretive paradigm.

4 The type of research: Two types of research have been identified in the literature. The first is empirical, based on experimentation or observation which seeks evidence. Such research is often conducted to test a hypothesis [http://library.manor.edu/tutorial/empiricalresearch.htm]. Empirical research sometimes depends on the context of the area under investigation, which is different from one situation to another. Some constructs and variables are validated and confirmed in one set of circumstances, but they are likely to differ if they are investigated and tested in another. The second type is theoretical research (i.e. conceptual), which aims to provide a new understanding of the phenomenon by constructing logical, arguable and reasonable connections and relationships between concepts that are relevant to the phenomenon where these concepts have already been proven and developed. Theoretical research is designed independently of any context.

Based on the above criteria, Tables 2.2 and 2.3 show the result of examining and reviewing previous research contributions on the security of e-commerce. Table 2.2 represents the studies sorted from the oldest (2000) to the most recent (2007), and shows the participant perspectives, the main contributions of these studies and the research methods and types used. There is another participant perspective besides those of the customer and the organisation (or, for that matter, of both together), namely that of the researcher. Studies of this type have no participants, whether
customer or organisation, but the researchers themselves give their assessments of security by considering both (e.g. Sharma & Yurcik, 2004; Knorr & Rohrig, 2001) or just the customer (Furnell et al., 2005).

<table>
<thead>
<tr>
<th>Author</th>
<th>Participant</th>
<th>Contribution</th>
<th>Research method</th>
<th>Type of research</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Antón &amp; Earp (2000)</td>
<td>Organisation</td>
<td>Implementing systematic mechanism for determining and assessing security and privacy requirements at early stage of e-commerce SDLC (requirement analysis)</td>
<td>Not mentioned</td>
<td>Theoretical</td>
</tr>
<tr>
<td>2 Turner et al. (2000)</td>
<td>Customer and security experts</td>
<td>Investigating factors affecting perceptions of security and privacy on e-commerce website</td>
<td>Qualitative</td>
<td>Empirical</td>
</tr>
<tr>
<td>3 Knorr &amp; Rohrig (2001)</td>
<td>Researcher’s opinion relative for both*</td>
<td>Framework for the analysis of security requirements of business processes in e-commerce</td>
<td>Experiment</td>
<td>Theoretical followed by empirical</td>
</tr>
<tr>
<td>4 Salisbury et al. (2001)</td>
<td>Customer</td>
<td>Providing evidence of impact of web security perception on intention to purchase online</td>
<td>Survey</td>
<td>Theoretical followed by empirical</td>
</tr>
<tr>
<td>6 Kesh et al. (2002)</td>
<td>Organisation</td>
<td>Framework for analysing e-commerce security as process to design and assess security infrastructure</td>
<td>Not mentioned</td>
<td>Theoretical</td>
</tr>
<tr>
<td>7 Chellappa (2002)</td>
<td>Customer</td>
<td>Showing that the perceived privacy and security are the main determinants of trust in e-commerce transactions</td>
<td>Survey/questionnaire</td>
<td>Theoretical followed by empirical</td>
</tr>
<tr>
<td>8 Suh and Han (2003)</td>
<td>Customer</td>
<td>Identifying and showing the impact of customer’s perceptions of security controls on trust and e-commerce acceptance</td>
<td>Survey/questionnaire</td>
<td>Theoretical followed by empirical</td>
</tr>
<tr>
<td>#</td>
<td>Author(s)</td>
<td>Type</td>
<td>Methodology</td>
<td>Findings</td>
</tr>
<tr>
<td>----</td>
<td>------------------</td>
<td>--------------------</td>
<td>--------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10</td>
<td>Hutchinson &amp;</td>
<td>Organisation</td>
<td>Implementing Systematic Secure</td>
<td>for e-business security revealed in risk management process.</td>
</tr>
<tr>
<td></td>
<td>Warren (2003)</td>
<td>Customer</td>
<td>Methodology for Internet Banking</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Ruppel (2003)</td>
<td>Organisation</td>
<td>Showing evidence that ability of</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>organisation to control and secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>is a factor influencing e-commerce</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>implementation and success</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Sharma &amp;</td>
<td>Researcher's</td>
<td>Evaluating perceptions of security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yurcik (2004)</td>
<td>opinion relative</td>
<td>features of e-tax websites</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>to both*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Sengupta et al.</td>
<td>Organisation</td>
<td>Implementing Systematic Secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(2005)</td>
<td></td>
<td>Methodology in e-commerce as lifecycle</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Nilsson et al.</td>
<td>Customer</td>
<td>Identifying factors influencing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(2005)</td>
<td></td>
<td>customers' perceptions of security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>and trust in online banking</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Yenisey et al.</td>
<td>Customer</td>
<td>Identifying factors influencing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(2005)</td>
<td></td>
<td>customer perceptions of security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>in e-commerce</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Furnell et al.</td>
<td>Researcher's</td>
<td>Showing that there is lack of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(2005)</td>
<td>opinion relative</td>
<td>understanding by the end users of</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>to customer*</td>
<td>potential threats and of security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>technology used to protect against</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>them in e-commerce. Advising by</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>simplifying the technology,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>increasing the usability, and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>educating the users.</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Singh (2006)</td>
<td>Customer</td>
<td>Showing evidence that ease of use,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>convenience and usefulness and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ability to control increase</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>customers' perceptions of security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>in online banking</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Pennanen et al.</td>
<td>Customer</td>
<td>Exploring customers' perceptions of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(2006)</td>
<td></td>
<td>security, risk and trust</td>
<td></td>
</tr>
</tbody>
</table>
Table 2.2: Analysis of existing frameworks

* This means that the study involves no participants (i.e. customer or organisation), but the researchers give their conceptions of security by considering both [3] [12] or just the customer [16].

Table 2.3 shows the contributions of previous research in terms of the relation between the participants' perspectives and the applied research types/methods. It shows where the majority of the studies are focused. 'X' signifies gaps; however, some of these combination are inappropriate. One example would be the carrying out of research based only on the researcher's perspective (which means that no participants are employed) by the application of quantitative and qualitative methods. The number of studies concentrating on the customer's perspective was eight; those focusing on the organisational perspective numbered seven; and there were two combining both. Finally, there were three studies from the researcher's perspective.

<table>
<thead>
<tr>
<th></th>
<th>Quantitative</th>
<th>Qualitative</th>
<th>Quantitative and qualitative</th>
<th>Theoretical</th>
<th>Empirical</th>
<th>Theoretical and empirical</th>
<th>No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer perspective</td>
<td>[4][7][8]</td>
<td>[15][18][17]</td>
<td>[14]</td>
<td>X</td>
<td>[14][15][18]</td>
<td>[4][7][8][17][20]</td>
<td>8</td>
</tr>
<tr>
<td>Researcher's Perspective</td>
<td>[3][12]</td>
<td>X</td>
<td>X</td>
<td>[16]</td>
<td>[12]</td>
<td>[3]</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 2.3: Previous contributions by considering the relation between the participant perspective and the research type/method
2.10 Implications of the Analysis

Based on the above analysis, it can be said that the most amount of work has been conducted on customers' perceptions of security and risk. Some of these studies have proposed research models to be validated empirically and are quantitative in nature. Much research that has been done empirically tend to be quantitative, in particular that dealing with the customer's viewpoint, so a more qualitative focus is required in order to provide a richer understanding of the security perceptions and practices implemented on e-commerce websites. Further empirical work is needed to investigate the implementation of secure methodologies on e-commerce websites and to identify the factors influencing their implementation and development. Some of the earlier studies were theoretical and others were empirical. In general, all theoretical proposals can be tested and validated by carrying out empirical research. There is an obvious deficiency of research based on the critical paradigm. Very little work has investigated the customer and organisation together, so a useful contribution can be made by combining customer and organisational perspectives to investigate and identify empirically the effectiveness of security in e-commerce in order to reduce the gap between what is implemented by organisations and what is perceived by customers. This will enable to obtain a better understanding of security from the combined perspectives. The present study emerged to cover this gap.

2.11 Proposed Research Model

In response to the previous work surveyed in Sections 2.9 and 2.10, the researcher proposes an initial model of the effectiveness of e-commerce security as shown in Figure 2.7. The components of this model come out as a result of analysis the literature review (see Sections 2.7 and 2.8). This model considers the main participants in e-commerce; the customers and the organisations. With respect to the former, the perception of security is the central concern, while for the later, organisational and technical factors predominate.

The researcher believes that the effectiveness of security in e-commerce cannot be assured without the perception of security from the customer viewpoint on one hand and the implementation of security solutions by organisations on the other. If the customer is aware of security features in e-commerce but the organisation does not provide sufficient security solutions in the website, then there is no effective security; rather, there is a requirement to apply
solutions which satisfy the customers' needs. Similarly, if the organisation implements the best technical solutions that provide full security, without the perception and awareness on the part of customers that the website is secure, then these technical solutions mean nothing. Therefore, both perspectives are vital and complementary in ensuring effective security in e-commerce.

Figure 2.7: Initial proposed research model showing the factors influencing the effectiveness of e-commerce security
2.12 ICT and E-commerce in Jordan

This section provides background information about Jordan and outlines its recent development of Information and Communication Technology (ICT) and of e-commerce. It also reviews the key research previously carried out in Jordan, which shows that security is one of the main concerns for customers and organisations engaged in e-commerce, and that there is no research in Jordan focuses on e-commerce security from customer and organisational perspectives.

2.12.1 General information about Jordan

The Hashemite Kingdom of Jordan is situated in the Middle East and has a population of 6 million, 91% of whom are literate [www.infoplease.com/ipa/A0107670.html]. Jordan has been ranked 57th of 122 on the Network Readiness Index in the Global Information Technology report 2006-2007 (www.weforum.org/pdf/git/rankings2007.pdf). This assessment is based on a composite of three components: the environment for ICT offered by a given country, the readiness of the community’s key stakeholders (individuals, businesses and governments) to use ICT and the usage of ICT amongst these stakeholders. Jordan is mentioned in the Guinness Book of World Records (GBWR, 2001) (www.openarab.net) as having the highest number of Internet cafés located in a small region, which is in the city of Irbid. One street, 500 metres long, has more than 200 Internet cafés, which indicates a strong trend towards increased usage of this technology.

2.12.2 ICT development in Jordan

As reported by McConnell International, LLC (2002), with regard to e-readiness Jordan’s ‘e-leadership’ is rated medium to high compared to other countries in the world. According to this report, many conditions are present for the conduct of e-government and e-business. E-leadership, in this context, refers to the scope and nature of government and organisations effort to promote the networked world within the country and to promote the country as a regional or global centre in the networked world. Promoting ICT in Jordan has received support from his Majesty King Abdullah II, from government ministers and from business leaders. who have worked to set goals and strategies for the adoption of ICT in Jordan. His Majesty perceives ICT as the greatest potential to Jordan’s future success and growth.
In 2000 the government of Jordan made ICT a national priority. This decision was translated into what is known as the ‘REACH’ initiative, supported by both public and private sectors, whose goal is to develop “a vibrant, export-oriented, and internationally competitive ICT sector that can successfully attract investment and generate high value jobs” [www.intaj.net]. The REACH initiative was devised by the Information Technology Association of Jordan (INTAJ) and supported by the Ministry of ICT to develop the IT sector in Jordan, with a mission to promote and advance the Jordanian software and IT service industry in the global market. Intaj has grown from 53 organisations in 2000 to over 143 in mid-2006. Members of this association include companies working in Jordan in the fields of software development, support and application; telecommunications companies, value added assembly organisations and companies that distribute ICT products and services [www.intaj.net].

The Ministry of ICT initiated an e-government program in September 2000. The aim of this program is to enable businesses and citizens to obtain better (i.e. faster, more accessible, and less costly) services, to increase the government performance and efficiency, and to ensure transparency in government procedures and processes [http://www.moict.gov.jo/MoICT/MoICT_Initiative.aspx]. This initiative is still in progress. So far, the Jordanian government has 95% of its ministries online, all of these with full information about services, the ability to download forms and applications, and the ability to communicate with citizens and businesses via email (i.e. publishing stage). However, online governmental transactions (i.e. the transactional stage of e-government) to making secure payments for a service and tax, has not yet been achieved (Elsheikh et al., 2008).

The application of ICT in Jordanian business, industry, schools, universities, government departments and households is clearly occurring (Sahawneh, 2002). An e-learning initiative was begun in 2002 and has been implemented and supervised by the Ministry of Education and the Ministry of Higher Education and Scientific Research. The initiative comprises two tracks: e-education in schools and e-education at university level. In schools, the programme aims to introduce IT courses within the curriculum and to facilitate the required infrastructure. As a result, computers and the Internet are used in schools and have been connected through the schools network. In addition, IT, e-commerce and programming language courses are now taught
in secondary schools. Another development of ICT at the schools level is the EDUWAVE project, which has been deployed in schools to provide access to an e-portal for students, teachers and parents. This allows access to student data, all courses and grades via a central webpage [www.escwa.org.lb/wsis/reports/docs/Jordan_2005-E.pdf].

At the tertiary level, all public universities have completed their fibre-based campus networks. Distance learning activities have been initiated among some universities [www.escwa.org.lb/wsis/reports/docs/Jordan_2005-E.pdf] and some have recently set up wireless networks. There are 20 universities in Jordan offering degrees in IT subjects and more than 15 colleges preparing students to work in the IT sector. E-commerce courses also are taught in universities. Computer and Internet skills courses and one programming language are compulsory in Jordanian universities for all students in most of the faculties.

At government level, an ICT literacy programme for 20,000 government employees commenced in 2004 and staff have been trained to the International Computer Driving Licence (ICDL) level [www.escwa.org.lb].

To increase dissemination of computer and Internet facilities among citizens, Jordan Telecom has launched a ‘PC@every-home’ initiative in 2004, offering packages consisting of a personal computer, software, modem and dial up or ADSL access. The package includes delivery, warranty and Internet help disk for support; and, to encourage people to purchase, its price is estimated to be at least 40% lower than the market price, making it suitable for people on low incomes, as payments start at £15 per month spread over three years [http://www.escwa.un.org/WSIS/reports/docs/Jordan_2005-E.pdf]. A recent government initiative in 2007 was to provide a laptop for each university student, again at subsidised cost, starting at £10 per month.

An informal Internet survey was conducted in 2007 by the Jordan Telecom Company concerning landline telecommunications, to explore customers’ preferences. Asked if they would like to pay online, of the 741 respondents, 79% said that they would like to pay bills online, whereas 21% said that they preferred to pay physically [http://www.jordantelecom.jo]. This suggests that many
people have the ability and willingness to engage in e-transactions.

E-commerce awareness has been achieved through the establishment of an E-commerce Information Center (EIC) in the Amman Chamber of Industry (ACI) in December 2000. The EIC is responsible for executing the rolling out of the training programmes, and for providing guidance and support to the private sector with regard to the implementation of e-commerce systems (Sahawneh, 2002). The Electronic Business Development Activity (EBDA) is a national initiative supported by the European Commission and executed by the EIC at the ACI in order to address the dissemination of e-commerce awareness in the business community of Jordan and to encourage firms to introduce IT into their activities (Sahawneh, 2002).

In Jordan, most business organisations have websites to promote their products and services and to contact their customers (Titi, 2005). Several Jordanian companies have deployed e-commerce applications, including online payment, which has been adopted by firms in fields such as transport and delivery (e.g. Royal Jordanian Airlines and Aramex), commodities, flowers, confectionary, pharmaceuticals, car and hotel reservations and auction websites. Other companies provide the ability to pay bills online for such services as mobile and landline telephone networks. However, websites providing facilities for such e-transactions are still very few in numbers.

Many banks provide online services such as Internet banking, e-transactions and transfers. There are several methods of payment, including Visa, MasterCard, American Express, Maestro debit card and prepaid Internet shopping cards such as CashU for limited amounts.

Taken together, the developments and initiatives set out above indicate that Jordan has, and continues to become a technology friendly country that is familiar with ICT initiatives (Mofleh et al., 2008).

2.12.3 Previous e-commerce studies in Jordan

According to Aladwani (2003), Internet security was ranked the first concern of customers and business managers in Arab counties, such as Jordan in regard to the use of e-commerce. The following studies of e-commerce and e-banking adoption are of particular relevance to Jordan.

A study, conducted by Sahawneh (2002) among 31 organisations using survey method, found that many factors hinder e-commerce success in Jordan, based on the viewpoint of the participant’s organisations. The first is cultural resistance, which prevents the consumer from using the Internet for trade with unknown and/or unseen parties. Other influencing factors include trust, risk and security. He states there is an absence of security and legal mechanisms to protect transactions and consumers from deceit. In addition, there is a lack of awareness in organisations of e-commerce benefits. He found that language is another limiting factor, because the local language is Arabic and the majority of websites are in English. A limitation of Sahawneh’s study was that it investigated only the opinion of companies. Customers were not consulted, so it is difficult, for example, to judge whether they had problems with language or to assess their level of knowledge about e-commerce websites. However, this study was conducted in 2002, and e-commerce has progressed substantially in the subsequent six years since the study. For example, many websites now support two languages, especially those that are initiated from Jordan and other Arab countries.

In contrast, another study was carried out by Alsmadi (2004) to investigate the attitude of Jordanian customers towards using the Internet for online shopping. It had two important results: firstly, most Jordanian consumers are likely to have enough knowledge and skills to use such Internet services. Secondly, the issue of the security of online transactions was a key factor limiting people’s willingness to make greater use of online shopping.
Al-Sukkar (2005) conducted research into the adoption of Internet banking in Jordan: he found that among the main concerns of customers and banks were security and privacy. Siam (2006) also reports that the majority of banks in Jordan that had introduced online services agreed that confidentiality and privacy were necessary for the success of the electronic banking business.

Titi (2005) conducted empirical research to investigate the adoption of e-commerce by Small Medium Enterprises (SMEs) within Jordan. He found that most of the major barriers were concerned with government regulations, such as concerns about privacy and data security, and the lack of legal and business laws regulating e-commerce. Privacy and security issues were found to be among the main barriers to the success of e-commerce, besides other factors such as customers' readiness, awareness and knowledge, which influenced the adoption of e-commerce. Titi reports that most of the respondents agreed that ensuring security would help in the adoption of e-commerce and influence their decision to do so. However, the study did not specify whether the nature of security was considered in terms of perceptions, of security technology and infrastructure, or of something else.

According to a report prepared by the Peppers & Rogers Group (2006) to assess e-readiness in Jordan compared with sixteen other countries, Jordan has so far performed well with respect to the ICT sector, with respect to connectivity and infrastructure, human capital and innovative capacity in the IT industry. It did, however, identify a perceived gap in security and privacy in relation to e-commerce.

Al-Qirim (2007) conducted a single case study to explore the adoption of e-commerce in a Non-Governmental Organisation (NGO), the Jordan Chamber of Commerce (JCC). The interviewed staff of JCC reported as stating that the concept of e-commerce is not yet widespread in Jordan. In respect to security, they mentioned some incidences of misuse of the Internet among the organisation's employees, introducing harmful viruses to the network. The study indicated that there was no web security service in Jordan covering e-commerce infrastructure. Where establishing SSL in Jordan would require huge investments; the JCC is reported to deal with the VeriSign certification authority in order to have the SSL feature in its payment gateway. Al-Qirim (2007) states that the current unavailability of an e-payment gateway in Jordan was a
barrier to successful e-commerce. While the study provides useful information for NGOs and explores useful issues regarding e-commerce, the researcher believes that it has some weakness. Firstly, the case study is unrepresentative, not merely in terms of population and sample, but in regard to the subject of the adoption and diffusion of e-commerce in Jordan. NGOs and non-profit organisations have different objectives and considerations from commercial firms, while the basis of e-commerce for buying and selling services and products entails profit and competition. Finally, all interviewees were JCC employees, while the customers' viewpoints were not investigated.

Prior research into the adoption of e-commerce and Internet banking in Jordan has reported many factors that hinder such developments. The researcher considers it wise to investigate each factor separately in depth, in the hope that solving difficulties, making improvements and obtaining insight into each factor will enhance the adoption of e-commerce.

According to Rowley (2000), it can be said that the first and second stages of e-commerce development have been largely adopted in Jordan. Currently, most organisations have websites to promote their products and services and through which their customers can contact them. However, there is not yet a widespread adoption of the third and fourth stages, where the risk increases and the security features are required for online payment systems, for example. Security is a consistent barrier to the adoption and implementation of e-commerce for customers and organisations. Therefore, this research aims to facilitate the adoption of e-commerce by exploring the nature of these security concerns, both guiding by previous literature approaches and by exploration of fieldwork.

2.13 Summary and Conclusion

This chapter has provided the reader with the theoretical basis of this research. It has explored the current research on e-commerce security from the IS perspective and provided a framework for the analysis of the prior research. As a result, an initial model is proposed which summarises the existing literature on e-commerce security (see Figure 2.7). This chapter has also highlighted some gaps, which justify the conduct of the present research. As the target of this investigation is Jordan, it can be said that Jordan has made valuable progress in the ICT sector, but in regard to
e-commerce, adoption and growth are still hindered by factors which notably include security. Therefore, once sufficient security is provided and perceived to be in place, the adoption of e-commerce should improve. In Jordan, no previous research has considered e-commerce security from both the customer and organisational perspectives. Thus, this research is the first of its nature to shed light on this issue. It investigates the adoption of e-commerce from a security viewpoint, because it is an important and consistently influential factor in its success. In short, the study explores the nature of security in e-commerce from both customer and organisation perspectives within Jordan.
Chapter 3: Research Methodology

This chapter explains and offers a justification of the research paradigm and methods that will be adopted in this research. It is organised into five sections. Section 3.1 discusses the differences among the IS research paradigms, which are the interpretive, positivist and critical paradigms. Section 3.2 considers these in respect of IS security. Section 3.3 presents the different research methods, Section 3.4 discusses the case study research method in more detail and Section 3.5 provides the justification and validation of the adoption of this research method. Finally, a summary and conclusion is provided. This chapter provides the basis for the next chapter which sets out the analytical approach adopted in this research. The two chapters together constitute a complete account of the adopted research methodology.

3.1 Research Paradigm

IS research can be classified according to the philosophical assumptions underlying it. The first is ontological, depending on whether the empirical world is considered to be objective and to exist independently of human observers, or subjective and constructed through human action and belief. Also, there are assumptions about the nature of knowledge (i.e. epistemology), how it is created and evaluated, and the relationship between theory and practice (Orlikowski & Baroudi, 1991). Orlikowski & Baroudi (1991) and Klein & Myers (1999) distinguish three paradigms of IS research: positivist, interpretive, and critical.

3.1.1 Positivist Paradigm

The positivist paradigm was originally used in natural sciences such as biology and physics. Its adherents view the researcher as independent from the research objects and context, and consider the world to be an objective construct in which the researcher just observes the phenomena of interest without affecting them. Positivist researchers believe that reality is objectively given and can be described by measurable variables, which are independent of the researcher and any human action and experience (Orlikowski & Baroudi, 1991). They assume that there exist a priori, fixed and given relationships among phenomena that are typically investigated with structured instrumentation (Orlikowski & Baroudi, 1991).

Orlikowski & Baroudi (1991, p.5) classify IS research as positivist “if there [is] evidence of
formal propositions, quantifiable measures of variables, hypothesis testing, and the drawing of inferences about a phenomenon from the sample to a stated population”.

Positivists are concerned with the empirical testability of theories. The relationship between theory and practice in the positivist philosophy is mainly a technical one, where the researcher evaluates or predicts actions or processes, but he/she cannot elicit subjective opinions from the people performing them (Orlikowski & Baroudi, 1991). Because the aim of positivist researchers is to explain and predict an external reality instead of people’s action, this requires researchers to ignore aspects of social reality (Orlikowski & Baroudi, 1991).

Positivist research is considered by some to have the strengths of high reliability and generalisability, because it uses large samples (e.g. via the use of survey methods) and provides statistical results (Gable, 1994). However, Collis & Hussy (2003) state that the main criticisms of positivist research are (1) that it is impossible to consider people as being separate from their social environment, so that they cannot be understood without examining the meanings, opinions and motivations they ascribe to their own actions; and (2) that the results of such research may neglect the more relevant and interesting meanings.

3.1.2 Interpretive Paradigm

Interpretive research has been used in the social sciences and is made relevant here by the recognition that IS research involves people as a key part of the interaction with the system. Interpretive research is said to have become noticeably much more important in the IS field in the early 1990s (Walsham, 1995).

Interpretive research supposes “that people create and associate their own subjective and inter-subjective meanings as they interact with the world around them” (Orlikowski & Baroudi, 1991, p.5). These people construct a reality which is a ‘social product’ through interaction, which it is unreasonable to attempt to understand independently of the individuals concerned, including the researcher who is part of the phenomenon (Galliers, 1992). Hence, interpretive researchers try to understand phenomena by accessing the meanings that are given to them by participants. Interpretive researchers attempt to understand how and why individuals, through their social interaction and participation in the world, give certain subjective meaning to that world. It is
important to recognise this subjectivity and expect that each person has different views of the world.

Interpretive research considers that scientific knowledge is not captured in hypothetical deductions but through the understanding of the human and social interactions by which the subjective meaning of the reality is constructed (Walsham, 1995). The interpretive paradigm deems that human language and actions should be used both to describe the social practices and to form those practices.

Orlikowski and Baroudi (1991, p.5) state that studies are classified as interpretivist if "the intent of the research [is] to increase understanding of the phenomenon within cultural and contextual situations; where the phenomenon of interest [is] examined in its natural setting and from the perspective of the participants; and where researchers [do] not impose their outsiders' a priori understanding on the situation".

Like positivist research, interpretive research is subject to criticism. Orlikowski and Baroudi (1991, p.18) note that the interpretive paradigm "neglects to explain historical change; that is, how a particular social order came to be what it is, and how it is likely to vary over time". Other criticisms of interpretive research concern the bias of the researcher and the participants, and the inability to generalise its results to the extent that is possible in positivist research. However, this point is less damaging if it is considered that the generalisation arising from interpretive research should be not from the sample to the population, but rather from the analytical to the theoretical (Yin, 1994); thus the analysis of the results of interpretive research leads to generalization through the development of concepts, the generation of theory, the drawing of specific implications and the contribution of deep insight (Walsham, 1995).

3.1.3 Critical Paradigm

Critical researchers believe that social reality is historically constructed and that it is formed and reformed by people (Myers and Avison, 2002). The critical research paradigm supposes that objective observation is impossible and that all knowledge is generated from or justified by the social context, so there are clear similarities between the critical and interpretive research
paradigms (Khazanchi & Munkvold, 2003). The basic difference between critical and interpretive research is that the former is transformative in its nature, focusing on changing the status quo, while interpretive research can be seen as more neutral and descriptive (Khazanchi & Munkvold, 2003).

For Klein and Myers (1999, p.3), “IS research can be classified as critical if the main task is seen as being one of social critique, whereby the restrictive and alienating conditions of the status quo are brought to light”. The main characteristic of critical research is emancipation. It aims to “free human subjects from oppressive regimes within societies and within the institutions that constitute them” (McGrath 2005, p.88).

Critical research seeks to explain social inequities and how individuals can take actions to change injustices. For example, the critical researcher may investigate why gender inequality exists in IT workplace where the motivation is to understand and challenge power that produces inequity (Trauth and Howcroft, 2006). Indeed, critical researchers can investigate the concept of empowerment, by asking questions about the relation between the employees and the management, and whether the management grants the employee power to promote their potential and provides the employee decentralized decisions or does it just oppress their potential and not emancipate them. Therefore such research can investigate the nature of the contradictory between the management and the employee and suggest how employees could try and overcome their social and economical conditions to better their situation.

The main problem of critical research in IS seems to be that it does not fulfil its self-professed objective of emancipation (McLean and Stahl, 2007). In addition, the researcher’s lack of power in relation to the organisations under investigation has an important influence on the level to which the researcher can progress in seeking for emancipation and transformative action (McLean and Stahl, 2007). Even when the researcher has the power to achieve that, then political and ethical issues emerge. Khazanchi & Munkvold (2003) summarise the key differences among the types of IS research paradigms as shown in Table 3.1.
<table>
<thead>
<tr>
<th></th>
<th>Positivist</th>
<th>Interpretivist</th>
<th>Critical Research</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ontological Assumptions</strong></td>
<td>• ‘Naive Realism’, in which an understandable reality is assumed to exist, driven by immutable natural laws. The true nature of reality can only be obtained by testing theories about actual objects, processes or structures in the real world.</td>
<td>• Relativist: the social world is produced and reinforced by humans through their actions and interactions</td>
<td>• Historical realist; social reality is historically constituted; human beings, organisations and societies are not confined to existing in a particular state</td>
</tr>
</tbody>
</table>
| **Epistemological Assumptions** | • Verification of hypotheses through rigorous empirical testing  
• Search for universal laws or principles  
• Tight coupling among explanation, prediction and control | • Understanding of the social world from the participants' perspective, through interpretation of their meanings and actions  
• Researchers' prior assumptions, beliefs, values and interests always intervene to shape their investigations | • Knowledge is grounded in social and historical practices  
• Knowledge is generated and justified by a critical evaluation of social systems in the context of researchers' theoretical framework adopted to conduct research |
| **Relationship between Theory and Practice** | • It is possible to discover universal laws that govern the external world | • Generative mechanisms identified for phenomena in the social sciences should be viewed as 'tendencies', which are valuable in explanations of past data but not wholly predictive of future situations | • Generalization in critical research focuses on the 'totality' of relationships |
| **Role of the Researcher** | • Objective, impartial observer; passive, value-neutral | • Interactive: the researcher interacts with the human subjects of the enquiry, changing the perceptions of both parties | • Transformative: initiating change in social relations and practices, helping to eliminate the bases of alienation and domination |

Table 3.1: Comparison among IS research paradigms
Source: Adapted from Khazanchi & Munkvold (2003)
3.2 Research paradigms in IS Security

Different research paradigms (i.e. those described in the previous section of this chapter) have been adopted within IS security, which can be classified according to the IS research paradigms (Dhillson & Backhouse, 2001; Siponen, 2005a). Dhillson & Backhouse (2001) states that, within IS research, few security approaches adopt radical humanist principles (i.e. the emancipation of human beings) meaning the critical research paradigm. However, they criticise the critical paradigm in IS security as the emancipated employee of an organization may lose interest in the core business, introducing significant risks. The following subsection examines some IS security research that has been conducted from positivist and interpretive perspectives.

3.2.1 Positivist paradigm in IS Security

According to Dhillson & Backhouse (2001), the information security literature based on this paradigm is classified under three headings: checklists, risk analysis and evaluation.

Checklists are one of the most popular methods for addressing the security of technical systems. They help in identifying every possible control that may be implemented. Security checklists have been constructed as an evaluation guideline, enabling an analyst to check a computer-based system and determine the necessity of existing controls and the possibility of implementing new ones. Dhillson & Backhouse (2001) criticise this method as paying narrow attention to the observable (technical details) and checking the measures, without considering the social nature of problems.

Risk analysis methods consider that negative events can be prevented and how information systems can be made secure, if countermeasures are developed and implemented in a logical and sequential way. The fundamental principle in evaluating risk is to analyse the possibility of threat and vulnerability. Critics of the use of risk analysis state that the estimation of probability is inappropriate for evaluating security risks, because threats are invariably random in nature and if the original estimation is incorrect then the resulting probability is inaccurate (Dhillson & Backhouse, 2001).
Evaluation is another research approach which is used to measure security. For example, there have been established IS security standard evaluations such as the British Standard for information security management BS7799, which is used to address security management issues in organisations. In addition, in the UK, for example, the Department of Trade and Industry has produced a series of ‘Green Books’ which aimed to provide standards for commercial computer security. IS security standards tend to be international and official, and are typically expressed in terms of imperatives or goals (what should be done); they are also used by many organisations. Evaluation methods are often initially developed for military use and then translated for commercial use. According to Dhillson & Backhouse (2001), this causes problems, because the social world of a defence environment is significantly different from that of the social world of commercial environment.

3.2.2 Interpretive paradigm in IS Security

The main aim of this paradigm is to appreciate the social implications of computer-based information systems and to increase awareness of the cultural aspects of IS security (Dhillson & Backhouse 2001). A socio-technical view of IS security that requires the integration of technical solutions with organisational aspects (Siponen, 2005b) is included in interpretive research. IS security planning and soft system methodologies are approaches that emphasise organisational, cultural and human issues in managing IS security and which are based on interpretive assumptions (Siponen, 2005a). Siponen and Heikka (2008) state, by referring to several authors, that the soft system methodology used for IS security planning give emphasise to the role of user participation in secure IS design and development to (1) utilise the user’s knowledge of the activities of the organization and (2) to increase users’ awareness and commitment to the designed IS security solutions. They also define secure IS planning methodology as consists of three elements: a security risk planning model, an awareness program and a countermeasure matrix. The five stages of the secure IS planning model to be followed – (1) detection of security problems, (2) risk analysis, (3) generation of alternatives, (4) decisions and (5) implementation. The awareness program and countermeasure matrix are integrated into these stages.

As mentioned in Section 3.3.1, the evaluation and checklist approaches to the study of IS security are positivist in nature and assume that IS security can be seen as an object independent
of the social context. According to Dhillson & Backhouse (2001) and Siponen (2005), however, risk analysis can also be studied under the interpretive research paradigm to develop managerial guidelines for an organisation. In this case, both the social context and the actions of individuals are involved. For example, the misuse of a system by an employee causes a risk, the investigation of which entails the involvement of the employee. The awareness of IS security by participant users, and the abuse and misuse of IS belong to the security domain, which involves people's perceptions and falls within the interpretive paradigm (Siponen, 2005), where a subjective viewpoint is adopted and the meanings assigned by people are identified. In addition, the roles of people, actions, goals and policies in an organisation are investigated under this paradigm to specify organisational security requirements (Dhillson & Backhouse, 2001).

3.3. Research methods

Research methods are usually classified into quantitative and qualitative. Quantitative research is objective in nature and concentrates on measuring phenomena; it involves the collecting of numerical data and analysing it by applying one or more statistical tests (Collis & Hussy, 2003). Quantitative research methods are used to prove or disprove hypotheses by determining the dependent and independent variables. They do not help the researcher to discover any new variables emerging during the investigation. Survey and experiment are examples of quantitative research methods, which are typically belonging to the positivist paradigm. The following paragraph provides brief descriptions of the principal quantitative research methods.

Survey is usually used as a quantitative method where a sample of a phenomenon is drawn from a population and studied to make inferences about that population. This method may be implemented through questionnaires and/or structured interviews. There are two major types of survey: descriptive surveys are concerned with identifying and counting the frequency of specific populations, while in analytical surveys the intention is to determine whether there is any relationship between different variables (Collis & Hussy, 2003). The data gathered in a survey is analysed using statistical techniques. However, the survey method provides only a 'snapshot' of the situation at a certain point in time and does not provide information about the implications of the data (Gable, 1994).
Experiments are conducted in a laboratory or in a natural setting in a systematic way that permits considerable control by allowing the researcher to eliminate certain variables or keep one or more variables constant. Experimental methods permit causal relationships to be identified and the aim is to manipulate the independent variables in order to observe the effect on one or more dependent variables (Collis & Hussy, 2003). Criticisms of this method include the claim that laboratory settings do not reflect the real environment and that there is a lack of realism in concentrating narrowly on certain variables (Collis & Hussy, 2003).

Qualitative research methods were developed in the social sciences to enable researchers to study social and cultural phenomena (Myers & Avison, 2002). Qualitative research is more subjective in nature and involves examining and reflecting on meanings and perceptions in order to gain an understanding of social and human activities (Collis & Hussy, 2003); and it involves collecting and analysing texts and meanings. Action research, ethnography, grounded theory and case study are qualitative research methods that are typically associated with the interpretive paradigm. However, a case study as a qualitative research method can be either positivist or interpretive (Myers & Avison 2002). The following paragraph provides brief descriptions of the principal qualitative research methods.

**Action research** is method which assumes that the social world is constantly changing and that the researcher and the research itself are part of this change. Action research aims to intervene into a situation in an attempt to bring about a change to that situation and to monitor the results. It therefore has two principal goals: to solve the given problem for the client and/or the community, and to contribute to science by making a change in the organisation or community (Collis & Hussy, 2003). There is debate about this method in regard to the collaboration between researchers and practitioners, with the latter participating in the research process. It is argued that this feature of this type of research means that the method can be considered as research ‘consultancy’ or ‘journalism’ (Gummesson, 1991); that it produces practical knowledge but neglects the scientific discipline (Baskerville and Wood-Harper, 1996).
Ethnographic research is a method in which the researcher uses socially acquired and shared knowledge to understand the observed patterns of human activity, aiming to interpret the social world in the same way that the members of that world do (Collis & Hussy, 2003). Ethnographic research comes from the discipline of social and cultural anthropology, where an ethnographer is required to spend a significant amount of time in the field (Myers & Avison, 2002). For example, in the area of IS design and evaluation, some research collaborative work has taken place between ethnographers on one hand and designers, IS professionals, computer scientists and engineers on the other (Myers & Avison, 2002). In order to achieve such collaboration, the researcher would need to select an appropriate organisation where the research problem is interesting and where he can build a high level of trust with those people that he wants to interact with in order to collect the required data. These conditions are difficult to achieve for many researchers.

Grounded theory is a qualitative research method which seeks to develop theory that is grounded in data, systematically gathered and analysed (Myers & Avison, 2002). It was devised by Glaser and Strauss (1967) for use in health science, but has since been used by researchers in IS and other disciplines. It uses a set of procedures to develop an inductively derived grounded theory about a phenomenon. The purpose of grounded theory is to build theory that clarifies the area being studied (Collis & Hussy, 2003). The major difference between grounded theory and other qualitative research methods is its specific approach to theory development, where it is suggested that there is a continuous interplay between the data collection and data analysis stages (Myers & Avison, 2002). Glaser and Strauss (1967) suggest that the researcher who uses grounded theory should enter the research setting without predetermined ideas as far as possible. This requires a long time period of collecting data from scratch and with no theory in mind. In opposition to this, Allan (2003) states that there has to be some agenda for research by interview, because busy people in industrial and commercial organisations expect meetings to have agendas and research topics scoped and identified. Time and resource constraints forbid fuzzy investigation. Grounded theory is used as the analytical basis of this research; specifically, it is the Strauss and Corbin (1990) approach which is adopted and which will be explained in detail in the next chapter.

A case study is a qualitative research method. This method is explained in more detail in the following section.
3.4 Case Study research

The case study method is used frequently by IS researchers, and many consider it appropriate for investigating IS phenomena (Benbasat et al., 1987; Orlikowski & Baroudi, 1991; Walsham, 1995; Darke et al., 1998; Alkout & Khalfan, 2004), as it helps to understand the problem in its natural setting.

Benbasat et al. (1987) lists three important reasons why the case study method is suitable for IS research:

1. The researcher can collect data and obtain evidence from a natural setting, then generate theories from practice.
2. The case study research method enables the researcher to answer ‘how’ and ‘why’ questions.
3. The case study method is an appropriate way to research an area in which few previous studies have been carried out.

Yin (1994, p.13) defines case study research 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”. According to Benbasat et al. (1987), a case study employs multiple methods of data collection to gather information from one or a few entities (e.g. persons, organisations) contained within the problem scope. Benbasat et al. (1987) list the main characteristics of case studies as shown in Table 3.2.

Case studies can be either positivist or interpretive (Walsham, 1995; Darke et al., 1998). Positivist case studies are designed and evaluated according to the criteria of natural science research, with controlled observation, deduction and the ability to generalize (Lee, 1989). In contrast, interpretive case studies are not concerned with repeatability, but focus on the principles of the interpretive paradigm (Darke et al., 1998). The researcher does not view himself as an observer from distance; rather, he shares the concepts and interpretations with the informant (Walsham, 1995). Researchers use case studies to test existing theory or to generate and develop new theory (Yin, 1994; Darke et al., 1998); and sometimes the research question shifts from theory testing to theory building during the research (Eisenhardt, 1989).
The phenomenon is examined in a natural setting;
Data are collected by multiple means;
One or few entities (person, group, or organisation) are examined;
The complexity of the unit is studied intensively;
Case studies are more suitable for the exploration, classification and hypothesis development stages of the knowledge-building process: the investigator should have a receptive attitude towards exploration;
No experimental control or manipulation are involved;
The investigator may not specify the set of independent and dependent variables in advance;
The results derived depend heavily on the integrative powers of the investigator;
Changes in site selection and data collection methods could take place as the investigator develops new hypotheses;
Case research is useful in the study of "why" and "how" questions because these deal with operational links to be traced over time rather than with frequency or incidence; and
The focus is on contemporary events.

Table 3.2: Main characteristics of case study
Source: Benbasat et al., 1987

3.4.1 Design of the case study research
Defining the research questions is the most important step to be taken before conducting an empirical research study. Yin (1994) claims that case studies are a particularly robust method to answer 'how' and 'why' questions. Some 'what' questions, where they are exploratory in nature, can also be the basis for conducting a case study (Yin, 1994).

Yin (1994) states that research propositions direct the researcher to focus on what kinds of information to collect. These propositions emerge from the literature and existing theoretical constructs. Identifying previous constructs or factors guides the researcher to form the preliminary design of theory-building (Eisenhardt, 1989). Eisenhardt (1989) emphasises the importance for researchers of recognising that it is impossible in the case of theory-building research to start with a 'clean theoretical slate', but that researchers should identify prior variables without predetermining the relationships among them; they should not be restricted to those alone, as sometimes new variables are found during data collection and need to be taken into account in reforming the theory.

After identifying the research propositions and questions the researcher needs to specify the case
and unit of analysis (Benbasat et al., 1987; Yin, 1994). A case may be a project or system (e.g. a geographical information system, IT governance or a management strategy such as outsourcing, recruiting or an IT position) (Paré, 2001). Its focus may be on individuals, groups and/or entire organisations (Benbasat et al., 1987). In some cases an individual person is the case being studied and the individual is the primary unit of analysis (Yin, 1994).

Single or multiple cases can be studied. According to Yin (1994), a single case is appropriate if the study is revelatory, exploring a situation previously inaccessible to scientific investigation. This represents a critical case for testing a well-formulated theory in order to confirm or challenge it; and a unique single case may meet all conditions for testing the theory. According to Benbasat et al. (1987), multiple case studies are desirable when the intent of the research is description, theory building and theory testing.

Yin (1994) identifies six sources of qualitative evidence in case study research:

1. Documents: e.g. letters, memoranda, agendas, administrative documents, newspaper articles, or any document that is related to the investigation.
2. Archival records: e.g. organisational records and charts, survey data and financial records.
3. Interviews: these can be of the form face to face or focus group. The researcher should prepare before carrying out interviews, and focus on the specific questions to be asked, whom to look at or talk with, where, when, about what and why. The questions also could be unstructured or semi-structured questions.
4. Direct observation: the researcher observes actions within the field environment.
5. Participant-observation: the researcher obtain insight into interpersonal behaviour
6. Physical artefacts: e.g. tools, instruments, computer output, emails, or some other physical evidence may be collected during the study as part of a field visit (Paré, 2001).

The ability to use different sources of data gives the researcher richer information about the topic of the research than may be available from just one source. However, Walsham (1995) asserts that interviews constitute the primary data source for interpretive case studies.

Yin (1994) proposes two methods to increase the reliability of case study research: the use of a
case protocol and the development of a case study database. A case study protocol is a document containing more than the interviews; it also sets out the procedures and general rules that should be followed by the researcher, and is prepared before the data collection phase (Yin, 1994). The protocol comprises an overview of the case study project (objectives, issues, topics being investigated) in order to communicate to the reader the general topic of research and the purpose of the case study. It includes also field procedures (credentials and access to case study sites, sources of information) that specify who should be interviewed and how access is to be gained to the right people; and ensure that there are adequate resources available, such as time, paper, and tape records, and schedule of the required data collection activities. Case study protocol comprises interview protocols which specify the issues to be discussed with the respondents and questions to be kept in mind during the interview. The other method proposed by Yin (1994) to increase reliability is the use of a case study database which includes raw material such as interview transcripts, researcher’s field notes and documents collected and survey material, coded data; memos and other analytic material.

3.4.2 Criticisms of case studies
Interpretive case studies can be criticised for the tendency to be biased towards both the researchers and the interviewees. The main function of the researcher is to minimize the level of bias in his work, according to Lubbe (2003), who lists a number of obstacles to obtaining unbiased evidence from observers. First are the difficulties encountered by respondents in being able to remember accurately. Individuals may also feel inhibited in disclosing important feelings; and they may have misgivings about revealing information that might reflect badly on them or their superiors. There are some actions that can be taken to ensure adequate safeguards against such bias. For example, interim reports should be submitted to the people from whom data was collected and their critiques included in the final report. Secondly, the use of the chain-of-evidence technique allows an external observer—the reader of the case study, for example—to follow the derivation of any evidence from initial research question to the conclusion of the study (Yin, 1994).

Another common criticism is the inability to generalise from a single case study. Yin answers that case studies are generalisable to theoretical propositions and not to populations or universes.
the case study does not aim to represent a sample and the aim of the researcher is to provide “analytical generalisation” rather than “statistical generalisation”. As noted also by Walsham (1995), the purpose of generalisation from a case study is to extend and generate concepts and theory, and to draw specific implications.

Another weakness is that the availability of suitable case study sites is limited because organisations are not always willing to participate in such research (Darke et al., 1998). A final criticism is related to the analysis of large amounts of qualitative data where there is no standard analytical approach (Darke et al., 1998).

3.5 Justification for selected research paradigm and method

This research explores the perceptions of security issues in e-commerce from the viewpoints of both customers and organisation (i.e. IT staff and business managers). This involves understanding the meanings and actions of the participants within the social world that they construct; and this world cannot be understood without knowledge of the beliefs and interpretations of people concerning it. An account of perceptions requires social and human factors to be understood, and this can only be achieved through interpretive research. Many IS researchers consider case study to be an effective method of IS research (Benbasat et al., 1987; Orlikowski and Baroudi, 1991; Walsham, 1995; Darke et al., 1998; Alkout & Khalfan, 2004), within which this topic of research (e-commerce security from the two perspectives) lies.

Because there have been no previous studies of security in e-commerce in Jordan, where the phenomenon is complex and contemporary, the case study research method is appropriate, as stated by Yin (1994) and Benbasat et al. (1987).

Interpretive case study research helps the researcher to understand phenomena in depth without narrowly defining certain predetermined constructs to be tested, then accepted or rejected. Rather, it gives the researcher insight into people’s actions and attitudes in regard to an issue, so allowing new issues to emerge. These provide a richer picture than a survey, which can only give answers to questions which are pre-specified by the researcher from the literature. Furthermore.
the aim of this research is to understand rather than to quantify a phenomenon.

Positivist quantitative methods assume that concepts and issues are known in advance and predefined from literature, which is not appropriate when investigating a phenomenon within a setting where it has not been investigated before. Even though the researcher has predefined concepts, he must adopt a flexible approach to develop and add new constructs as they emerge. Interviews are to be used as the main source of data to explore the participants’ perceptions of e-commerce security. However, using a case study, as Yin suggests, the researcher can collect data from different sources within organisations, observing and scanning artefacts such as e-commerce websites. The examination of reports, security policies and documents will constitute a rich source of data relevant to understanding the phenomenon.

Three other interpretive research methods should also be considered here: action research, ethnography and grounded theory. Action research projects are collaborative in nature. This means that there is collaboration between researcher and practitioners in order to fulfil objectives and solve human and organizational problems in real contexts. Action research requires the researcher to belong to a real organisation and to contribute to actual projects. As a result, s/he can give his/her opinion and can participate in and affect organisational decisions in order to change the current situation, which is inapplicable in this research. Furthermore, if the researcher is an employee of the organisation or a member of the project team, a number of ethical dilemmas may emerge from the conflict between the two roles, as researcher and as expert or technical participant. Thus, the duality of purpose may cause a problem in action research, related to the confidentiality of information provided and to political issues (Marshak and Heracleous, 2005).

The ethnographic method requires the researcher to stay a long time with the organisation in order to observe the human activities within it. This method focuses on understanding and interpreting the observations; it is not unlike participant observation in this respect. While in the case study method other sources of data are required, such as documents and artefacts (e.g. e-commerce websites). The main difference between case study and ethnographic research is the

60
extent to which the researcher submerges himself or herself in the life of the social group under investigation (Myers, 1999). The extra time that is needed in ethnographic research means that the best time to do it is probably during one's doctoral studies (Myers, 1999). Indeed, it is very time consuming, even if it is supposed that only one ethnographic study is conducted.

Grounded theory suggests that the researcher should have no predetermined ideas when collecting data (Glaser and Strauss, 1967). Indeed, it is undoubtedly not possible to investigate specific working practices in Jordanian organisations without some focus or goal to guide the work therefore there has to be some agenda for research by interview. However, as stated before that case study research does not provide a systematic way for analysing data. Thus, grounded theory was chosen to be used as a method of analysis of the qualitative data (Strauss and Corbin, 1990) which are collected from the present case study. The next chapter will explain the use of grounded theory in a way which is compatible with case study research, by justifying the use of Strauss and Corbin’s (1990) approach.

3.6 Conclusion
To summarise, the phenomenon of e-commerce security cannot be understood independently from interactions between customers and organisational stakeholders or without making sense of their meanings, so a positivist view that considers the reality of the world to be independent and isolated as an object is not appropriate in this research. It is therefore concluded that the interpretive case study method is appropriate in attempting to understand this phenomenon and to answer the research questions, and that interviews are a good way to collect the majority of the intensive data required. The next chapter will elaborate the grounded theory procedures and justify their use with the case study method, thus completing the account of the research methodology adopted in this study.
Chapter 4: Using Grounded Theory for Data Analysis

This chapter provides an elaboration of the use of grounded theory as a method of data analysis. The first section offers an overview of its use in IS. Section 4.2 discusses the two approaches to grounded theory, while Section 4.3 explains the procedures and techniques of grounded theory as a method of data analysis. Section 4.4 justifies the use of the Straussian approach in combination with the case study strategy to construct a methodology emerging from this integration, while Section 4.5 provides the criteria for evaluating the adopted research methodology.

4.1 Grounded Theory Overview

Grounded theory has been used by many IS researchers since the beginning of the 1990s (see for example Orlikowski, 1993; Urquhart, 2001; Fernández et al., 2002; Linden and Cybulski, 2003; Allan, 2003; Sorrentino and Virili, 2005; Hansen and Kautz, 2005; Coleman and O'Connor, 2007). It is becoming increasingly popular in IS research, as there is a widely held belief that it is a reliable method by which to investigate social and organisational phenomena, although it is still relatively new to this field (Hughes and Jones, 2003), having been first applied to IS research about thirty years after its introduction by Glaser and Strauss in 1967.

The general goal of grounded theory is to generate theories derived from data in order to understand the social and organisational context. Strauss and Corbin defined it as is a “qualitative research method that uses a systematic set of procedures to develop an inductively derived grounded theory about a phenomenon” (Strauss and Corbin, 1990, p.24). However, Hekkala (2007) indicates that grounded theory has been used in IS research both as a research method (by, among others, Urquhart, 2002; Jones and Hughes, 2004) but that it has also been sometimes used as a research methodology (by researchers including Orlikowski, 1993; Goulding, 1999; Goede and Villiers, 2003). Hekkala (2007) states that those who use it either as method or as a methodology do not soundly and logically demonstrate and justify their use of this theory for either of those purposes. The current researcher defines method as a procedure or technique used to collect and/or analyse data, whilst a methodology refers to the entire research process, from the identification of one or more research questions and the selection of a research method through to the formulation of the findings and results, in which the entire process is
based on certain philosophical assumptions (ontology and epistemology).

4.2 Grounded Theory Approaches

Grounded theory was propounded by Glaser and Strauss (1967), whose combined work can be considered as the first version of this theory. Strauss and Corbin (1990, 1998) subsequently developed and extended the original theory, in a form which later faced criticism from Glaser (1994). The divergence between the two original authors leads to what are commonly termed the Glaserian and Straussian approaches to grounded theory (Hekkala 2007).

In the IS field, many researchers have applied grounded theory without even mentioning that there are two distinct approaches. Hekkala (2007) confirms this by giving examples of papers (e.g. Orlikowski, 1993; Galal and McDonnel, 1997; Lubbe and Remenyj, 1999; Lehnmann, 2001; Rowlands, 2005) where there is no statement as to the variant of grounded theory being adopted. Thus, identifying the attributes of the two approaches is essential in order for researchers to decide at the outset which approach is more appropriate to their research and which to adopt. Onions (2006) highlights the major differences between the two approaches as shown in Table 4.1.

The role of existing literature within research activities is clearly different between the two approaches. Specifically, Glaser (1992) asserts that the literature should not be examined before commencing the study, so as to avoid constructing prior assumptions and beliefs which might unconsciously bias the researcher. He writes of “a need not to review any of the literature in the substantive area under study” (Glaser, 1992, p.31) and later contends that the “pre-study literature review of QDA [Qualitative Data Analysis] is a waste of time and a derailing of relevance for the GT [Grounded Theory] study” (Glaser, 2004, p.9). Glaser (1992) supposes that the research problem and questions are only discovered once coding begins and that “the research question in a grounded theory study is not a statement that identifies the phenomenon to be studied” (p.25).
Glaserian Approach | Straussian Approach
---|---
Beginning with general wonderment (an empty mind) | Having a general idea of where to begin
Emerging theory, with neutral questions | Forcing the theory, with structured questions
Development of a conceptual theory (abstraction of time, people and place) | Conceptual description (description of situations)
The theory is grounded in the data | The theory is interpreted by an observer
Inductive method | Inductive-deductive method
The researcher is passive, exhibiting disciplined restraint | The researcher is active
Data reveals the theory | Data is structured to reveal the theory
Coding is less rigorous, a constant comparison of incident to incident, with neutral questions and categories and properties evolving. Take care not to ‘over-conceptualise’, identify key points | Coding is more rigorous and defined by technique. The way of making comparisons varies with the coding technique. Labels are carefully crafted at the time. Codes are derived from ‘micro-analysis which consists of analysis of data word-by-word’
Two coding phases or types, simple (fracture the data then conceptually group it) and substantive (open or selective, to produce categories and properties) | Three types of coding: open (identifying, naming, categorising and describing phenomena), axial (the process of relating codes to each other) and selective (choosing a core category and relating other categories to it)
Regarded by some as the only ‘true’ Grounded Theory Methodology (GTM) | Regarded by some as a form of Qualitative Data Analysis (QDA)

Table 4.1: Grounded Theory Variants
Adapted from Onions (2006)

In contrast, Strauss and Corbin (1990) acknowledge that there should be some survey of the literature before the fieldwork commences and that the researcher enters the research area with some knowledge of the phenomenon being studied. They believe that the literature can be used to derive questions that the researcher desires to use in field work. They state that “the research question in a grounded theory... tells you what you specifically want to focus on and what you want to know about this subject” (Strauss and Corbin, 1990, p.38). They also state that the
literature directs so-called theoretical sampling and is helpful for theoretical sensitivity (see Section 4.3 for definitions of these terms). Furthermore, it can be used as a way for supplementary validation, meaning that after the researchers finish their research, they could show how it differs from previous works or whether they include common findings.

Hekkala (2007) states that the Straussian approach is an inductive-deductive one; deductive in that the researcher has some preconceived theories and hypotheses, and inductive in that it enables new concepts to emerge.

Glaser (2002) criticises the Straussian approach, stating that it forces a theory from the data because it forces data into a predetermined paradigm model of relationships (i.e. cause, condition, context and consequence), rather than letting any theory emerge. In the Glaserian approach, the researcher does not have to find preconceived causes, consequences or action/interaction relationships (Glaser, 1992). According to him, this paradigm model is the aim of qualitative data analysis, termed by him a “full conceptual description”. For this reason, as stated by Hekkala (2007), Glaser claims that the approach of Strauss and Corbin (1990) can be considered only as a method providing techniques for data analysis, not a methodology. Glaser (2004) states that the original version of grounded theory (Glaser and Strauss, 1967) is a methodology, while the later versions are QDAs. Glaser (1992, 2002) maintains that the Straussian approach focuses on conceptual description by spending time describing the researched situation and categories without abstracting the time, peoples and places, while the original or classical grounded theory, as he calls it (Glaser, 2004), focuses on conceptual analysis by concentrating on conceptualisation and abstraction of data, generating conceptual hypotheses that can be applied to any relevant times, places and people. However, Strauss and Corbin (1990) also claim that a researcher who uses grounded theory should move analytically from description to conceptualisation at the selective coding stage, which is explained in the following section.

4.3 Grounded Theory Procedures

This section elaborates the Straussian approach procedures of analysis in order to show subsequently how these can be combined with the case study research method to form a viable research methodology. Hekkala (2007) notes that most IS researchers rely on Strauss and
Corbin’s (1990) book, which concentrates on providing techniques for researchers who want to use grounded theory.

Strauss and Corbin (1990) assert that the coding procedures in grounded theory are neither automatic nor algorithmic: “we do not at all wish to imply rigid adherence to them” (Strauss and Corbin, 1990, p.59). In other words, flexibility may be necessary in certain circumstances.

Briefly, the following sequence is followed in order to arrive at the research model (theory) which is grounded in the data:

\[
\text{Codes} \rightarrow \text{Concept(s)} \rightarrow \text{Categories} \rightarrow \text{Model (Theory)}.
\]

Coding is the key process in grounded theory (Strauss and Corbin, 1990). It begins in the early stages of data collection, after the first interviews and comprises three coding steps. Throughout this process, two analytical techniques are used. The first is constant comparative analysis, which is a continuous procedure of identifying conceptual categories and their properties emerging from data by continuous comparison of that data. The researcher needs to be sensitive, which means the ability both to identify what data is significant and to assign it a meaning. This sensitivity comes from experience, especially if the researcher is familiar with the subject under investigation. The literature review is another source of theoretical sensitivity (Strauss and Corbin, 1990), and so are the expressions of the interviewees themselves, in particular when they repeat the same phrases and concepts. The other technique is the asking of questions. Once the researcher has named the concept (event, idea, action) then he or she asks questions regarding such things as what it is and what it represents.

The three above-mentioned coding steps are open coding, axial coding and selective coding:

**Open coding** is “the process of breaking down, examining, comparing, conceptualizing and categorizing data” (Strauss and Corbin, 1990, p.61) by which concepts and their proprieties and dimensions are identified from data that are transcribed by the researcher. This can be achieved either line by line or by focusing on main ideas in sentences or paragraphs (Strauss and Corbin,
1990). Each code represents a word or sentence containing a meaningful idea, while a group of two or more codes forms a concept. A concept is an abstract representation of an event, object or action. In open coding, events, objects and actions are compared with others in terms of similarities and differences in order to give them, when similar, the same name. The name or label that is assigned to a category should be selected logically and usually seems to represent the data. A reading of the literature gives the researcher an initial set of concepts that can be used, but researchers should not be constrained by these concepts; rather they should focus on the words and phrases used by the participants themselves. It is in this way names are assigned to categories and the new concepts are defined (Strauss and Corbin, 1990).

**Axial coding** is the process of reassembling data that has been broken down through open coding. Essentially, it is the process of relating categories to subcategories. Categories are higher in level and more abstract than concepts, and are generated by constant comparison of the similarities and differences between such concepts. This is done by using what is called the 'paradigm model', which enables the researcher to think systematically about the data and their interrelationships (Strauss and Corbin, 1990). This model addresses the relationships between the categories by considering the following aspects:

1. **Causal conditions** represent incidents or events that lead to the occurrence of the phenomenon.
2. **Phenomena** represent the central ideas or events about which a set of actions/interactions are directed or handled. Their meaning concerns the extent to which the set of actions are related.
3. **Context** refers to specific properties related to a phenomenon. It represents a set of conditions under which action/interaction strategies (detailed below) are followed.
4. **Intervening conditions** can exercise influence by facilitating or constraining the action/interaction strategies within a particular context.
5. **Action/interaction strategies** are devised to manage, handle, carry out and respond to a phenomenon under a specific set of conditions.
6. **Consequences** are the outcomes of actions and interactions.
Selective coding is the process of integrating and refining the theory under building. The first step in integration is to identify the central or core category, which represents the main theme of the research. This central category, which must appear repeatedly in the data, acts as a master that pulls the other categories together to form an explanatory “whole picture” by using the paradigm model. In this step the categories are refined at a high level of abstraction and categories that need further explanation are given more descriptive details. This process of integration is not dissimilar to axial coding, except that it is done at a higher, more abstract level of analysis and the subcategories are linked to the core category. Finally, a storyline, which is a conceptualisation of a narrative description of the study’s central phenomenon, is analytically explained (Strauss and Corbin, 1990).

Sampling in grounded theory is based on theoretical sampling, on the basis of concepts that have been shown to have theoretical relevance to the developing theory. It is related to the sampling of new data based on the analysis of that initially collected from the first interviews, where the emerging concepts constantly guide the researcher as to the nature of future data, its sources and the issues to be discussed in subsequent interviews in order to develop the categories. The initial questions for the fieldwork are based on concepts derived from the literature (i.e. data gathered previously), which provides the researcher with a starting point and a focus; later, the sampling becomes more in-depth. Strauss and Corbin (1990) explain that the sampling should focus on incidents and not persons per se—in other words, collecting data about what informants do or do not do in terms of actions/interactions and their conditions and consequences. Mays and Pope (1996) states that:

“The purpose [of sampling in qualitative research] is not to establish a random or representative sample drawn from a population but rather to identify specific groups of people who either possess characteristics or live in circumstances relevant to the social phenomenon being studied.”

This purposive sampling is adopted in this research, where the researcher seeks rich information from individuals’ or groups’ experience, or behaviors that provide the greatest insight into the research question. The theoretical sampling mentioned-above is a form of purposive sampling (Patton, 1990). The researcher continues this process until the theoretical base is saturated, i.e. when no new ideas emerge regarding categories and their relationships.
4.4 Justification for using grounded theory and in particular the Straussian approach with case study research method

Fernández et al. (2002) state that grounded theory and case studies can be used in combination. However, this appears incongruous, as their preference for the Glaserian approach means that the researcher should not review any literature before the fieldwork, and the research question is based on the emergences of codes during data collection and analysis. This is contradictory to the case study research method developed by Yin (1994).

Hughes and Jones (2003) state that grounded theory is consistent with interpretive case studies which investigate social and organisational contexts. They suppose that there are some justifiable reasons for the use of grounded theory in interpretive case studies. Nevertheless, they do not show how and why the case study is consistent with grounded theory and could therefore be combined to form a methodology, and which variant of grounded theory is more appropriate.

Hughes and Jones (2003) also state that empirical work shows a discrepancy between the interpretive perspective and the grounded theory procedures by which they ought to be applied, since the procedures of coding, comparing, categorizing and saturating are consistent with a positivist and mechanistic attitude. However, Strauss and Corbin (1990) defend their position, stating that the procedures used in grounded theory are neither automatic nor algorithmic and that they do not compel the researcher to adhere completely to them. Furthermore, by using the techniques of constant comparative analysis and of asking questions for each code (concerning what it means and what it represents), interpretations are made by the researcher, especially when new concepts emerge; this is still falls under the interpretive assumption that the researcher is part of the research process.

In essence, there is a similarity between the case study strategy and the Straussian approach to grounded theory, as explained below:

- The case study strategy devised by Yin (1994) suggests that the researcher should start with a specified problem statement and a set of research questions and propositions. He states that research propositions direct the researcher to focus on what kinds of information to collect.
with no research propositions the researcher might be tempted to collect everything. These propositions emerge from existing literature. He furthermore refers to the literature review in order to develop the case study protocol which includes the research objectives and case study questions that are used as a reminder, rather than as the actual questions by which data is collected from the interviewees. This also agrees with Strauss and Corbin's (1990) approach that the researcher cannot start without any literature on the phenomenon that is being studied; nevertheless, the researcher is not limited by the literature and embraces the flexibility of accepting emergent ideas. Moreover, the research question in grounded theory should tell the researcher specifically what to focus on and what the researcher wants to know about the subject of research.

- Both case study and grounded theory use interviews as a technique for data collection (Allan, 2003), and both consider the interview to be the main source of data (Yin 1994; Walsham 1995; Strauss and Corbin 1990).

- A chief characteristic of case study research is the specification of the boundary and the scope of the research cases and the unit of analysis (e.g. organisation, group of people, certain system, activity); this is compatible with the grounded theory concept of theoretical sampling as mentioned by Strauss and Corbin (1990) where the criterion for selection of the cases and the unit of analysis in the case study is relevance, and theoretical sampling serves to seek in-depth information from the cases, and to discover and develop the concepts and theories.

- The generalisation of research findings by case study and grounded theory is similar in that the results of the research might be transferred to another context and situation with similar characteristics. Grounded theory aims to develop theories and concepts that can be generalised and applied to other situations. The generalisability of the grounded theory is partly achieved through a process of abstraction; the more abstract the concepts, the more theory applicability (Strauss and Corbin 1990). In the same way, Yin (1994) state that in case study research the researcher's aim is to expand and generalise theories: "analytic generalisation" rather than "statistical generalisation". Walsham (1995) specified this
analytical generalisation by the developing of concepts, the extending and generating of concepts and theories, and the drawing out of specific implications.

It can be said that the major difference between the case study and grounded theory is that the latter details the procedure of data analysis as discussed in the previous section, while the former includes pattern matching and explanation building, which is not as rigorous for analyzing collected data case studies. Indeed, one of the main criticisms of the case study is related to the analysis of huge qualitative data where there is no standard analysis approach (Darke et al. 1998). This, together with the compatibility assessment described above, provides a justification for integration the case study research method and (Straussian) grounded theory. This is the overall research strategy that has been adopted for the current research.

Grounded theory has been chosen since it clarifies the concepts and categories that emerge from the data. Grounded theory allows the researcher to fulfil the aims of this research; it assists in building a model at an abstract level to define the factors and the interrelationships between them which influence the effectiveness of e-commerce security. In other words, the analytical procedures of this method, particularly the processes of open, axial and selective coding, will allow the researcher to identify and explore the factors. Furthermore, this approach enables the researcher to be flexible and update his questions in order to identify new and emergent issues. Finally, it is compatible with interpretive case-based field studies, as justified above, and endorsed by IS researchers as appropriate for investigating human viewpoints and experiences, as this research seeks to do.

4.5 Criteria for evaluating the quality of research design

Yin (1994) has proposed a set of tests and criteria (validity and reliability) for evaluating the quality of a case study. Strauss and Corbin (1990) also define a set of criteria and a group of questions in order to ensure that concepts, categories and theories are fully developed and grounded. Yin’s (1994) criteria are not adopted in this research for evaluating the proposed methodology, which combines case study and grounded theory, because these criteria are suitable only for positivist quantitative research, not for interpretive qualitative studies (Golafshani, 2003). Since positivist research aims to test hypotheses and make predictions.
whilst interpretive research aims to understand phenomena within their natural settings and in terms of human insight, the criteria for evaluating the former are not appropriate for the latter. On the other hand, Strauss and Corbin’s criteria are used in evaluation, in particular of generated concepts and theory which are inappropriate for evaluating the whole research process. Because both case study and grounded theory are integrated under the umbrella of interpretive qualitative research, the combination of both as a methodology involves finding a mutual basis on which to evaluate that methodology. Lincoln and Guba (1985) provide a set of criteria that are designed for interpretive qualitative research in general, and their criteria evaluate the entire research process. These criteria are:

- **Credibility**, which demonstrates that the research was conducted in such a way that its subject was correctly identified. Credibility is enhanced by using multiple sources of data, by assigning to various respondents the concepts and meanings that have been gathered in order to find matches, by allowing participants to check their interview transcripts and give comments on them, by using data triangulation, and through prolonged engagement in fieldwork.

- **Transferability**, which shows whether the findings can be transferred to other situations. The generalisation in interpretive qualitative research is not deduction from small samples to large populations, but rather aims to show how certain methods can obtain the same results when they are transferred to other contexts with similar properties. This can be achieved by providing the reader with rich, detailed information of the context that has been investigated, and by concentrating on abstraction and conceptualisation.

- **Dependability**, which shows that the research process is systematic, well documented and traceable. This is achieved by clearly identifying the documentation of the methods and approaches used in the research.

- **Conformability**, which assesses whether the findings emerge from the data collected from cases rather than from preconceptions by showing raw data and demonstrating the steps of
the analysis leading to the extraction of the results and outcomes.

Figure 4.1 illustrates how grounded theory can be integrated with the case study research method to form the research methodology that is used within the present research and which follows the above clarification on the integration and compatibility. As shown in this figure, the researcher starts with a general research topic. In order to identify gaps, discover new areas of research or extend the existing body of knowledge, the researcher reviews the literature. Based on this review, the problem studied becomes more bounded and the research question is identified; this defines the aim of the research. The literature review helps the researcher to identify the relevant concepts and theories pertaining to the research question, and consequently models or a set of propositions (concepts) are proposed. These are not to be tested or validated, but rather serve to enhance theoretical sensitivity and sampling. The cases and units of analysis are selected for their relevance to the research question, and the research protocol is prepared including research questions to be asked in the field by considering flexibility and enabling new data to emerge. These data are collected principally from interviews, but possibly also from documents, observations and artefacts. In fieldwork, the interplay between data collection and analysis is processed simultaneously by identifying ideas emerging from the first interviews, so that the area under study becomes more focused as time progresses. At the same time theoretical sensitivity and sampling and constant comparison between data are taken into account finally results in that data becoming saturated, which is the point at which no new ideas emerge. A systematic process of coding begins once the empirical data has been gathered, at each step of which there are outcomes: codes and concepts, and categories and relationships between them. These ultimately form the research model. It could be that the resulting categories and relationships are not fully saturated, so a second round of data collection and analysis is initiated, which develop a new version of the research model. The entire process that results in this model is then evaluated according to criteria of credibility, transferability, dependability and conformability. Finally, the researcher may show the originality and the contribution to the literature by comparing the present research with the previous work and the initial model.
4.6 Conclusion

This chapter has provided a demonstration of the use of grounded theory, showing how the elements of case study and grounded theory are compatible. In particular, it has justified the use of the Straussian approach to grounded theory in conjunction with case study research as a methodology. Next chapter sets the methodology in application. It defines the research cases and unit of analysis, and case study protocol, elaborate the procedures and actions undertaken during the entering the fieldwork and gathering data.

Figure 4.1: Research design: Case study-Grounded Theory Methodology
Chapter 5: Data Collection Process

This chapter presents the procedures followed in this research, from the steps that preceded the fieldwork through to the entire data collection process. Section one gives an account of the selection of the case studies and Section 5.2 addresses the ethical issues. Section 5.3 presents the case study protocol and Section 5.4 describes the rationale for the use of the protocol and the initial research model shown in Chapter 2. Section 5.5 set out the actions undertaken during the early stages of fieldwork and Section 5.6 discusses the saturation procedures that were followed in order to end the data gathering process. The actual results of the fieldwork are then presented in Chapter 6.

5.1 Selection of the case studies

Understanding the nature of e-commerce entails the study of interactions between customers and businesses having e-commerce websites, as well as the IT providers who develop these. In a good case study, a particular group of defined individuals is specified. In order to understand the security concerns on e-commerce as perceived by the involved participants, two case studies were selected for the fieldwork. The first case constituted a group of individuals (n=15 participants) who are educated and experienced of Internet services, and some of them familiar with online transactions. The participant’s ages were between 20 and 35. The second case constituted a group of key people from several organisations, including managerial and IT staff from several business and IT companies (n=12). A description about these companies, and how many from each company participated, is provided in appendix G. The roles of the participants were not linked directly with the companies to keep the confidentiality of the participants (see Section 5.2 ethical considerations). In summary, this second group comprised three IT managers, three business managers, an e-business director, an IT Security manager, two software and web developers, an engineering support worker, and a customer support worker from an IT solutions company. The units of analysis in the two cases were the perceptions and viewpoints of these participants. Secondary sources were also used: two websites were scanned with the business participants, specifically (B2C) and (C2C) e-commerce websites, and four documents were provided by the participants, the first related to the achievement of an organisation in introducing the new systems in their website, the second related to the architecture and components of the
secure electronic payment system developed by an IT solution provider, and the third and fourth related to e-commerce and e-government policies and initiatives in Jordan.

It is important to mention that the participating staff members were selected from more than one organisation, because if data had been gathered from only one organisation, that some relevant data might have been missed, the research questions might not have been answered comprehensively and the study might not have produced a complete picture (since all the potentially relevant issues would be unlikely to emerge from work within a single organisation). For example, issues were expected to emerge from commercial companies which could not be found within the IT provider companies that are responsible for developing the e-commerce applications. In addition, the perceptions of security in e-commerce are likely to be different within the IT company that has developed a particular application from that within the organisation running its business through e-commerce and different again among customers, who are involved in its use but outside the business boundary. Therefore this approach enables a wide range of relevant factors to be examined from the viewpoint of many interested parties. Typically, the researcher specified the group of interviewees who appeared most relevant to the study and based on purposive sampling.

5.2 Ethical considerations

Although the ethical considerations in this research were minor, the researcher was very cautious in this respect from the beginning of the research process; the approval of the University’s Research Ethics Committee was obtained, since the research involved human interaction (see appendix B). The researcher informed the participants of the objectives of the project before asking them any questions regarding the study, and showed them an official letter obtained from the university confirming that the aim of gathering data was for scientific purposes only (see the text in appendix C). To ensure that the research followed ethical principles, the researcher sought the permission of all informants to record the interviews. Some accepted and others declined to do so; their wishes were respected.
No details are given in this thesis which would identify the participants themselves or the websites, for three reasons: firstly, to keep the confidentiality of the respondents, some of whom declined permission for their interviews to be recorded. Secondly, the present research is not intended to have a marketing research focus, presenting the services, products and history of the websites in a way which would promote them in a thesis whose aim is to provide a record of scientific and academic research. Thirdly, the researcher wishes to preserve the freedom to criticise and to present his own viewpoint, particularly in critical discussion, which may oppose that of the website or the interviewee concerned, and this can only be done effectively without explicit reference to specific company (i.e. no direct link between the participants and the companies was revealed).

5.2 Case study protocol

As noted by Yin (1994), using a case study protocol increases the reliability of the research so such a protocol was prepared before the fieldwork was undertaken (see Table 5.1). It includes the objectives and topics of the research, field notes, interview guides and the research questions to be used. The main focus of the interviews was on the customers and organisations (including IT staff and business managers) from whose perspectives this research draws its data. On the basis of the initial proposed research model shown in Figure 2.7, semi-structured questions were formulated to investigate customers’ perceptions of security, with a focus on the aspects identified in the research model, such as motivation, attitude towards security and knowledge of security in e-commerce websites—in other words, the views of customers in regard to security. This corresponds to the first sub-question of this research:

What is the customer’s view and perception of the security of e-commerce-websites?

The second group of questions, oriented toward the organisations’ staff, was also derived from the research model (Figure 2.7) that emerged from the analysis of the literature. It focuses on the view of the organisation in terms of technical, managerial and customer concerns with regard to e-commerce security. This corresponds to the second sub-question of this research.

What is the organisational view of the managerial, technical and customer concerns
regarding e-commerce security?

Yin (1994) mentions that the questions that are formulated within the case study protocol are principally aide memoires for the investigator, rather than actual questions for respondents, serving as reminders regarding the data that need to be gathered. The main purpose of these questions is to keep the researcher on track as data collection proceeds. In general, they were open in nature in order to enable the participants to supply their opinion freely.

Objective of the research

The main aim of this research is to investigate the factors that influence the effectiveness of e-commerce security in Jordan, and its focus is on the perception of security from the customer’s viewpoint, from that of the organisation in respect of customers’ security concerns, and from IT and business managers’ perspectives concerning the managerial and technical implementation of secure e-commerce websites. To obtain in-depth and relevant information on the research questions, a series of semi-structured interviews will be conducted, affording the informants the opportunity of supplying their opinions, knowledge and experiences of a wide range issues.

The key issues of the research are:

1. Identifying customers’ perceptions of security on e-commerce websites.
2. Identifying the managerial and technical considerations for implementing secure e-commerce websites.

The main research question is:

What are the factors and their interrelationships that influence the effectiveness of e-commerce security in Jordan?

The research addresses the following three sub-questions:

1. What is the organisational view of the managerial, technical and customer concerns regarding e-commerce security?
2. What is the customer’s view and perception of the security of e-commerce websites?
3. How can the organisational view and customer views on e-commerce
security be integrated into a coherent framework that provides guidance to all participants in e-commerce?

Field note
The fieldwork of this research took place in Jordan. The researcher obtained initial consent to meet key people from an IT provider companies who were responsible for developing e-commerce applications and businesses managers of a companies which had an e-commerce website; besides these, a group of Internet users was interviewed. The interviews were conducted in two cycles; the first took place from 15/6/07 to 22/7/07, the second from 1/4/08 to 1/6/08.

Interview guides
- The researcher will inform the interviewees of the time and the date of the interviews.
- The researcher will show the interviewees an official letter obtained from the university declaring that the data is being gathered for scientific purposes.
- The researcher will start with brief introduction to the company and the informants.
- The researcher will show participants the objectives of the research.
- The researcher will use an audio recorder and take written notes directly during the interview.
- The researcher will seek the permission of the informants to record the sessions.
- At the end of each interview the researcher will summarise the issues discussed and ask the informants to comment on what they have said if that is possible.

Customers' questions
- Have you ordered anything online or paid bills on the Internet?
- If not, why not?
- In your opinion, is using Internet for buying products safe and secure? Why/why not?
- Do you feel confident in the security of e-commerce transactions? Why/why not?
- What does security on e-commerce websites mean to you?
- What security features do you think should be required on e-commerce websites?
- Do you know how to check whether a certain website is secure or not?
Have you faced any problems on e-commerce websites?

Do you have experience or knowledge of security in e-commerce?

**IT and Business Managers’ questions**

- What is the extent of public acceptance of electronic commerce in Jordan?
- Do you think that people accept e-commerce as a secure channel for buying and selling? Please explain your opinion – how and why?
- In your opinion, what security measures should be required on e-commerce websites? Do you think we need security for every e-commerce website? What do you think of the current level of security on e-commerce websites?
- How do you build secure e-commerce applications? Do you follow certain processes? Can you explain that?
- What security tools and techniques do you use in e-commerce websites? Are there measures which you use to check? What are they?
- Do you take the security requirements into account when beginning an e-commerce development? How?
- Can you tell me what security procedures should be followed in order to build and develop secure e-commerce websites?
- Do you take the customer’s viewpoints and perceptions into consideration when developing e-commerce websites? Why? How?
- In your opinion, what are the concerns of customers regarding whether a website is secure or not?
- Do you think that top management influences the consideration of security functions as a priority in e-commerce? How?
- Is security in e-commerce websites considered as an enabler for your business? How?

Table 5.1: Case Study Protocol
5.3 The rationale for the use of the initial model and the case study protocol

The initial model that was presented in Figure 2.7 was not intended to be validated or tested, but to give the researcher a better understanding of the area of concern and to enhance the theoretical sampling and theoretical sensitivity (see Section 4.3). In addition, as the aim of this research is to extend the existing body of knowledge on e-commerce security, the initial model served to identify ways in which the results of this research could make a contribution and add new knowledge. In other words, a researcher cannot know whether he is adding new knowledge or extending the body of knowledge if he does not know what already exists. In addition, the present research provides a set of implications and a critical discussion of the results.

The researcher started by establishing the theoretical foundation of the study in order to guide the setting of the questions. As mentioned before, the case protocol was then used as a checklist or aide memoire to assist the researcher in discussing the issues with the informants. The interview questions set out in the protocol were developed continually as a result of new interesting ideas emerging from the interviews, such as security in EPS and outsourcing, responsibility issues and intangible indicators of security that influence customers’ perceptions.

One of the useful notions of qualitative research that the researcher utilised while gathering the data was to consider each interview as a pilot interview. The preliminary analysis of the first interviews informed the emergence of new issues to be discussed and investigated in the subsequent interviews. This capability is not available in quantitative research, where the researcher cannot know the result or where the data is leading until he has finished collecting and analysing the whole data set. Within qualitative research (i.e. grounded theory), the analysis of qualitative data begins with the collection of the first interview data, so there is constant interplay between collection and analysis.

5.4 Beginning the Fieldwork

The researcher arranged most of the interviews two months in advance, informing the interviewees of the issues to be explored and of the main aim of the research. He first contacted them by telephone and email. Examples of corresponding emails were kept in order to increase the research credibility (see appendix D). Having obtained the consent of the interviewees, the
researcher arranged a schedule time for meeting them. Each interview began by exploring the background, position and role of the informant. This was a good introduction from which to move smoothly to the core topic of the study.

Semi-structured interviews were used as the main research tool to obtain answers to the research questions, supplemented by documents and artefacts (e.g. e-commerce websites; n=2). The researcher utilised the set of questions shown in the research protocol in Table 5.1. However, the interviews were not limited to these questions, as the informants were allowed to add their opinions and beliefs freely, which led to the emergence of new questions and issues throughout the meetings. The websites of two commercial companies were scanned to identify their security features; in one case this was done while the business manager responsible was being interviewed, so that he could be questioned systematically on the services and features provided on the e-commerce website. This procedure also helped to ensure the credibility of data that was gathered during the interviews.

Some of the interviews were recorded on tape, but some respondents declined to be recorded. The researcher preferred to write notes during the interviews, even though he used a recorder in some of them, for two reasons: first, to give respondents the feeling that they were providing useful data, consequently giving them the opportunity to express their opinions and beliefs freely and comfortably while indicating that the researcher was aware of and interested in what they were saying. Secondly, this enabled the researcher to highlight the concepts and ideas from the earlier interviews, which were then discussed and explored in the subsequent interviews; in other words, the process of data collection and analysis ran simultaneously from the first interviews.

5.5 Data Saturation
The procedure adopted to decide when to cease collecting data, called data saturation (Glaser & Strauss, 1967; Strauss and Corbin, 1990), depends on four dimensions. Under the first, the researcher continued the interview process until the data that were being gathered consisted largely of repetition, with no new ideas emerging and no new insights gained. The second criterion was based on the research questions: once the results and findings were deemed sufficient to answer these questions, then the research objectives could be considered to have
been fulfilled. In addition, by using theoretical sampling, i.e. by interviewing the key relevant participants, the quality of the data collected was enhanced. The researcher attempted in advance of collecting data to meet the key people having experience and knowledge of the study issues. Finally, the researcher considered his supervisor's evaluation as another supportive procedure to ensure that the collected data were sufficient to meet the research objectives.

5.6 Conclusion

This chapter has set out the circumstances in which the data were collected, identifying the criteria for selection of the case to be studied, explaining the procedures for data collection and the associated ethical issues, enumerating the sources of data, producing the research protocols and describing the way in which the development and continuation of the data-gathering process was based on the emergency of new data. The gathered data at this stage is then passed to the next stage of the research, the stage of analysis, which is covered in the following chapter.
Chapter 6: Data Analysis

This chapter describes in detail the findings from the fieldwork conducted within Jordan and provides an analysis of the data gathered from both customer and organisational perspectives. The findings are presented in such a way as to show the reader, by giving examples of responses made by the participants, how the categories and concepts were grounded in the data, and how that they are a reflection on gathered data. The construction and assembling of concepts followed from a rational application of the grounded theory procedures described in earlier chapters. The categories, including the key concepts, are then shown in terms of interrelationships to form the final proposed research model.

6.1 Application of grounded theory procedures

The researcher has identified concepts and categories through applying constant comparative analyses between segments of data and the asking of continuous question - what does this piece of data mean? The researcher has provided examples which show how the data has been analysed, for example, an interview, conducted with a customer, was transcribed by the researcher and is provided in appendix A. The analysis of this interview started through transcribing the recording and then converting the voice dialogue into Arabic text, which was the language of the conversation. Then, the researcher translated the Arabic into an English version. The researcher asked two people, both native Arabic language speakers, to provide some validity that the two versions, Arabic and English, have identical meaning (confirmation letter signed by two people provided in appendix F). After that, the actual analysis started, by the author reading through the text line by line, and labeling significant words or key points. For instance, as presented in the transcribed text of the interview (provided in appendix A), when the researcher asked the customer the question: in your opinion, is using the Internet to purchase products safe and secure, and why? The participant responded:

“It depends, if the website that you would like to buy from gets the trust from the people ... and if you hear that people use a certain website and gain satisfaction and the website is good, then I think I would do” (Participant 1)

From this short excerpt above, specific keywords were highlighted through underlining, which
represents a certain code. The researcher reviewed the underlined keywords, such as "gets the trust from the people" and "hear that people... gain satisfaction", and asked himself what do these mean or represent; what is the viewpoint of the customer; are these codes important: do these codes provide insight into the researched questions; and what interpretations can be extracted from these codes? It can be identified, from this excerpt, that there is one important concept of 'trust', where the concept is itself is a code phrased by the customer. The researcher's experience and knowledge of previous literature guided him directly to the importance of this concept, and therefore, highlighted its significance. The other concept is "people's experience". This concept is extracted and understood from the excerpt "hear that people... gain their satisfaction". The researcher initially proposed the concept of 'people's experience' as a concept that could signify that users depend on other past experiences, and recommendations from others, when using certain websites; they would also use these when deciding whether a website was secure or not. Throughout this process, it appears that there are similarities in concepts, which can be grouped under one category. For instance, from the same interview, and as shown in appendix A, the concepts 'reputation' and 'commendation from people' have both also emerged from collected data. At this point, the researcher found that these concepts, namely 'trusted from people', 'commendation from people', and 'reputation' have similarities, thus they have been grouped under one category. The researcher also chose 'intangible features of security' as the name for the category, with a description presented for this in Section 6.2.3. Intangible features of security are not seen on the specific website and cannot be directly checked by users of a website. Intangible features are constructed by informal word-of-mouth communication among people; there are further concepts extracted from the interviews, which have the same meaning and proprieties as information provided in Table 6.1. The researcher continued this process until all possible concepts and categories were identified, and this resulted in the open coding stage being completed.

The next stage in the process is axial coding, where relationships between categories are identified. For example, the social communication category causes and constitutes a perception of tangible (security certificates) and intangible (reputation) security features. This relationship has been identified in the data also. Thus, the participant pointed out:

"I hear that a padlock at the bottom of the page means 'this website is secure' but I can't tell you if this actually is secure or not, but the main thing for me is what other
The above example demonstrated that people depend on what they hear from others when evaluating whether a certain website is secure or not. For example, past experiences with certain websites and success stories will encourage other people to try buying via e-commerce, and because of recommendations, concerns over security and credibility of a particular website will be quelled. Advice that is recommended is through informal word of mouth between individuals, when relating to checking the padlock on the secure website. At the axial coding stage, the concepts were refined and repetition reduced. More than one customer mentioned the same concept about websites: trust, reputation, recommendation/commendation of the website. The concepts and categories were also reassembled and sorted. For example, tangible security features and intangible security features were grouped together under one category named ‘tangible and intangible security features’.

At the final stage of selective coding, the researcher elicited the core category that was mentioned frequently by participants (customer and organization’s staff alike), whether this was implicitly or explicitly. Additionally, this links to other categories and represents the main area of the researched problem. The core category in the present research is “cooperative responsibility” as will be presented later. At this stage, the research model was constructed at a high level of abstraction, and the description of all identified categories and their relationships are presented in the following sections.

6.2 Results of analysis based on the customer perspective

Five categories which were identified from the analysis of customers’ responses are described in the following five subsections. It will be seen that some excerpts are quoted in one category and then re-quoted in another, because more than one meaning and insight can be extracted from one response.

6.2.1 User’s/Customers Characteristics

A set of concepts was identified from the customer’s responses: user’s experience, knowledge, practice, learning and experimentation. These are depicted in Figure 6.1, where the rectangle shape (unshaded) represents the name of the category, and the ellipses shapes represent the
concepts identified from data, which were grouped and linked to the category. Also within Figure 6.1, the direction of the arrow shows the direction of the cause-affect relationship, where the category influences e-commerce security effectiveness. Shaded rectangle represents the goal.

![Diagram](image)

**Figure 6.1: User Characteristics category influences on e-commerce security effectiveness**

All of the identified concepts reflect the characteristics of the users of e-commerce websites. Customer’s answers reflect the degree of security awareness that they have of such websites. The concepts; experience, knowledge and practice concern the means of dealing with the website and what must be known in order to determine whether that website is secure or not. For example, some participants reported that they had no knowledge of security issues and buying online:

* I don’t know what website security is. It is something experts do... it is something inside the system but me, I don’t know. (Participant 12)

* Well, the reason is, I have no experience in how to deal with the webpage that comes up when I select an item for purchasing. It asks for a credit card number and in fact I don’t have one. (Participant 5)

* The main problem for us is we are not used to using credit cards to buy stuff from the Internet. (Participant 3)

* I do not think there are websites in Jordan where you can use a credit card... are there? ... I don’t know. (Participant 11)

* I hear that a padlock at the bottom of the page means ‘this website is secure’ but I can’t tell you if this actually is secure or not, but the main thing for me is what other people say, because they have more experience of these websites than me. (Participant 1)

The last participant had no understanding of the meaning of security features on e-commerce
websites (e.g. the padlock symbol), so he depended on the experience of others. The level of each concept differs from one customer to another. A user who has a high level of experience and knowledge tends to use e-commerce with confidence; other users will not engage in this activity. Examples are given below of participants who claim to have knowledge and experience of e-commerce websites:

Yes, of course I have dealt with many websites like Amazon and eBay. I've bought many books. Honestly, I've found that is a convenient way to do shopping online and I feel I have the knowledge. (Participant 9)

I can say I have the minimum level of information about how to deal with e-commerce websites. You know, there are things everyone should know ... but me, I tried the first time and then I did it again because I had experience, but the first time the fear barrier was with me. (Participant 3)

One participant reported that knowledge and experience came with time and practice:

....also this comes through practice, which comes with time... it doesn't come suddenly all at once. (Participant 15)

Some users did not own credit cards but they claimed that they were able to perform online transactions and check security features on websites. For example, one participant, in response to the question “Have you bought anything online?” said:

Participant 8: No
Researcher: Why not?
Participant 8: I have no credit card
Researcher: Suppose you did have one, could you tell whether the website was secure?
Participant 8: Yeah, you have to buy from famous websites, and check their security certificate.

Another participant had a credit card but did not use it online because he had no need to:

Yes... I have one ...... but I haven’t seen anything I want to buy online. Maybe in future ..... Actually this depends on your need ...Once this need comes I will..(Participant 15)

Another participant claimed that people do not know what they should know, referring to the continuous learning process and his level of knowledge:

The problem is, people don’t know what they should know. Me too, I’m still learning. I can’t say I know everything. (Participant 3)

Another participant said that there was an imperative need to learn the relevant issues of using e-
Why I am learning is because sometimes you have no choice but to buy from the Internet, so you need to understand everything that's relevant. (Participant 9)

As for the following participant, his first experience of an e-commerce website drove him to say:

Yes... but I don't advise you to buy online because it is risky... really hazardous! (Participant 6)

In contrast, the next participant had a positive attitude based on his first experimentation and was likely to repeat it:

I tried the first time and then I did it again, because I had experience, but the first time the fear barrier was with me. (Participant 3)

It is clear that there are differences between the concepts that represent the user's characteristics; for example, learning is the process of obtaining knowledge, and utilising this knowledge in reality can be called practice or experimentation, but the main difference between them is that experimentation might occur without any prior knowledge, perhaps by chance or through the user's curiosity to try something new. Repeating practice and experimentation many times creates experience. From the earlier quotations, it will be noticed that some users clearly had no knowledge of security or even online buying. Some were learning, others claimed to have knowledge, while some felt they had experience after the first experimentation.

6.2.2 Security meanings and needs

The respondents expressed their understanding of security on e-commerce websites and their viewpoints on what security means were similar to some extent. Their responses tended to focus on the protection of private data such as credit card numbers, the accessing of such data only with the user's consent, and the receipt of the requested products and services without these being denied by the website. No model is provided for this category where the concepts and meanings presented in the following quotes are implicitly covered in other categories. Some of the participants expressed their views about security implicitly by providing accounts of how they would check the security of a website, for example:

In fact I have been a customer of this bank for a long time so I'm sure that the bank will not rob or trick me. But there are some instructions I should know as a customer to protect myself from other people. For example, the first time when I logged onto the system (website page) it told me I had to change my password after six months. I did
that but later on I tried to enter it... I forgot the new password. I tried many times and then the system asked me to contact my branch to activate my password because I'd entered the wrong password more than three times...... All of these processes are there to protect me so they are very concerned about security...do you think that a bank with a massive amount of money would let their customers lose their money? Of course not... so it is secure. (Participant 2)

This participant saw security as a tight set of procedures applied by the bank to protect his account, while others expressed their understanding of security explicitly, as mentioned in this section, by stating that:

Security means that my money is not lost and the website absolutely will send the item that I order and not fail to do that and they will deliver the item to my home on time. (Participant 3)

Well, security means once I've entered the security number which is on the back of my credit card no one can steal it (it is 3 numbers)..... It means that I get the goods I've ordered, not something else. (Participant 1)

Security for me means honest dealing between the customer and the company, like in traditional buying and selling. The company that respects its customers is well known and especially the big ones will implicitly provide the required conditions in order to do the transaction in a secure way. (Participant 5)

Security means that your private information is used only with your consent. For example, some websites when you buy from them, they pass your data on to others, and then you receive a lot of spam advertising emails... Some of them ask you if you would like to receive marketing emails. (Participant 10)

The following participant reports that he was reluctant to buy items from outside Jordan because he was not sure of receiving them, so he expressed the meaning of security by referring to the fear that the selling company would fail to send the goods that were ordered:

You know I purchased something from outside Jordan, available only on the Internet and not available in Jordan... I need it.... Actually, I was very reluctant ... I was afraid that it would not be delivered ... from America... they said it takes 10 days to 14 days... I phoned them and sent them lots of emails after 10 days to track the parcel..... Really, I was worried. (Participant 14)

6.2.3 Tangible and intangible indicators of security

The customer responses with regard to how to check the security of the website and what criteria to consider can be categorised into tangible and intangible features. Tangible ones are those technological security features of the websites that can be checked by users, such as https,
padlocks, security certificates and security symbols, while intangible ones are not seen on the website and cannot be directly checked over the website. They are affected by society in terms of communication and the environment: where the customer lives and what they hear from others, as well as their past experience. They include how well-known a company is and the reputation of its website. The awareness of such intangible features is constructed by informal word-of-mouth communication among people.

Tangible features need to be understood and checked by the customer over the website rather than captured through social communication; this involves having knowledge and experience of these features, such as knowing what a security certificate means and how to check if it has expired or not. Figure 6.2 represents the intangible and intangible categories that influence on e-commerce security effectiveness. Features that are related to each one of them are tabulated in Table 6.1. Theses were not presented in the diagram in order to maintain the simplicity.

Some customers indicated that the tangible indicators meant nothing to them, so the intangible indicators were prioritised, after which the tangible ones might or might not be checked. For example, the following participant indicated that the presence of a padlock on the website meant that it was deemed secure, but he did not rely on it totally; rather he depended on other people’s experience and recommendations.

*In fact this depends on what people say, for example I heard that a padlock at the bottom of the page means ‘this website is secure’... but the main thing for me is what other people say, because they have more experience of these websites than me.* (Participant 1)

Some respondents indicated that the presence of security features on the website and details of its policies, as well as the interface design, made them feel that it was secure. Examples from the
participants’ responses are the following:

I mean sometimes the website provides you information that makes you feel this website is secure and also through transferring between the pages, step by step until you get to the confirmation page, this gives me the feeling that they are serious and secure. (Participant 1)

If the website shows the customer a brief description of what security issues you should be aware of and understand then this makes the customer more trusting of the website. (Participant 11)

On the other hand, there are websites very formal, they have 'contact us', customer service call, this gives you an indication that it’s secure and reliable. (Participant 3)

I read their policy and all the information that’s relevant to the website if I have any doubt about it... transferring between the web pages as well gives you an indication that the payment process is secure. (Participant 9)

The participants reported that the involvement of a third party—one which is neutral and international, can act as an intermediary, is accepted by all parties and guarantees that security is provided—makes them perceive a website as secure and consequently encourages them to engage in e-commerce. Evidence of such involvement includes use of the third party’s logos and security certificates. For example, one participant said:

I think if there is a security company recognised internationally that shows that they have a list of websites registered by them as well as mentioning that they gave these websites a reference number, then the customer can go onto certain websites and check this reference number or the brand name of this company in the security company’s list... Not merely a stamp, but a reference number... This method makes buying over the Internet secure. (Participant 1)

...They should have a security certificate. (Participant 8)

Others also stated that receiving confirmation by email made them feel secure:

Well, some websites say that they have secure payment but this doesn’t mean it really is secure unless it’s provided by a third party. The availability of customer service to call them, and sending confirmation by email, all of these things make me feel the website is secure. (Participant 15)

Some participants perceived that reputation was equated to security; when they were asked how they would check whether a certain website was secure or not, participants sometimes referred to the trust placed in it by others and to depending on the rating scheme used on the website. For example:
Famous websites can be considered secure, like eBay and Amazon. These websites are under laws in these countries, such as the UK and the USA. (Participant 4)

It depends, some websites you can trust and some you can’t. Those that you can trust are international, recognised and secure, but if a website is not well known I don’t use it for buying. (Participant 9)

As I told you the famous companies provide security …. I suppose they do that because they respect their customers. Besides, they show details regarding the freight and delivery. (Participant 9)

I think the issue here depends on the website. I mean if the website is well known and rated by the users as secure and includes an actual address and telephone number, then this site is secure….. (Participant 13)

If I find payment via PayPal then I complete the transaction without any reluctance, because it is a well known company around the world. The reputation of the website through feedback and the rating by customers, and their experience with the website proves that the website is secure and credible. (Participant 11)

This last participant pointed to the familiarity of many users with electronic payment service providers such as PayPal. This was also asserted by another participant:

I haven’t heard any complaints about Amazon and ebay... you know why? Because these websites deals with largest companies in the world – like PayPal, which undertakes the security on the website, these websites [Amazon and eBay] pay millions for that. (Participant 4)

Reputation was also mentioned by other participants as the base that customers relied on if they wanted to buy online:

I think there is no way to say this website is secure or not – the only thing is the reputation of the company’s website. (Participant 1)

If I do... I do just from a company I have already dealt with or a company that has a good reputation in Jordan. (Participant 10)

Some participants highlighted the significance of the website’s identity, such as the banks and telecommunications companies in Jordan, saying that they would not use websites which were anonymous and had no real physical location:

I trust only the bank .... Suppose if anything happens, then I can go to them and rely on them, since they have an original physical address. (Participant 7)
In fact I have to deal with known people. (Participant 10)

Yes, I check the logo and security certificate...and their actual address, so if I have a problem I can go to them and complain. (Participant 13)

In fact I have been a customer of this bank for a long time so I’m sure that the bank will not rob or trick me. But there are some instructions I should know as a customer to protect myself from other people. For example, the first time when I logged onto the system it told me I had to change my password after six months. I did that but later on I tried to enter it... I forgot the new password. I tried many times and then the system asked me to contact my branch to activate my password because I’d entered the wrong password more than three times... All of these processes are there to protect me so they are very concerned about security. (Participant 2)

The last quotation also shows that from this participant’s perspective ensuring the security of his account is addressed by providing a strong password procedure, which increases his perception that the online bank is working to provide security for its customers. Some participants reported that the characteristics of the company (e.g. respected status and large size) would lead them to feel that it provided a secure website.

The company that respects its customers, if it is well known, and especially the large ones, they implicitly provide the required conditions in order to do the transactions in a secure way. (Participant 10)

I think the companies provide security in their systems when they build them. I mean these respected companies are surely not going to provide their customers with a way to pay online without taking security into account. (Participant 13)

Respectable companies are keen to provide complete systems to a high degree of accuracy, and therefore I believe the company because I feel that they provide high security... without any checking because I don’t know how to do that. (Participant 12)

One of the participants had not yet bought online but in his opinion there were certainly secure websites:

I hear that there are many people who buy over the Internet and some people buy and sell shares as well, so certainly it is secure, because there are people who do this, otherwise why do they buy and sell, if it’s not secure? (Participant 5)

Table 6.1 summarises all the tangible and intangible indicators of security from a customer’s viewpoint that were derived from the fieldwork. On close inspection, it may appear that several of the intangible indicators appear to be identical: for example, famous, well-known and recognised could be considered to be synonyms. However, the researcher has kept to the
customer’s exact phrases.

<table>
<thead>
<tr>
<th>Security features in e-commerce website</th>
<th>Category of security feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Padlock</td>
<td>Tangible</td>
</tr>
<tr>
<td>Security certificate</td>
<td>Tangible</td>
</tr>
<tr>
<td>Transferring between interfaces of the website</td>
<td>Tangible</td>
</tr>
<tr>
<td>Security policy</td>
<td>Tangible</td>
</tr>
<tr>
<td>Acknowledgment via email</td>
<td>Tangible</td>
</tr>
<tr>
<td>Third party symbols</td>
<td>Tangible</td>
</tr>
<tr>
<td>Physical address</td>
<td>Tangible</td>
</tr>
<tr>
<td>Brief description of the security issues that the customer should be aware of on the website</td>
<td>Tangible</td>
</tr>
<tr>
<td>Known identity (company has physical building, e.g. bank, and contact details)</td>
<td>Tangible</td>
</tr>
<tr>
<td>Support password system</td>
<td>Tangible</td>
</tr>
<tr>
<td>Well-known electronic payment gateway such as PayPal.</td>
<td>Tangible-Intangible</td>
</tr>
<tr>
<td>Famous</td>
<td>Intangible</td>
</tr>
<tr>
<td>International</td>
<td>Intangible</td>
</tr>
<tr>
<td>Recognised</td>
<td>Intangible</td>
</tr>
<tr>
<td>Trusted</td>
<td>Intangible</td>
</tr>
<tr>
<td>Well-known</td>
<td>Intangible</td>
</tr>
<tr>
<td>Formal website</td>
<td>Intangible</td>
</tr>
<tr>
<td>Respected company, large size</td>
<td>Intangible</td>
</tr>
<tr>
<td>Reputable</td>
<td>Intangible</td>
</tr>
<tr>
<td>Rating Scheme</td>
<td>Tangible</td>
</tr>
</tbody>
</table>

Table 6.1: Tangible and intangible security features of e-commerce websites from a customer perspective

6.2.4 Psychological aspect of security

The data appeared to show that there is a psychological aspect to security as far as the customer is concerned. Four concepts were identified in relation to this category: fears, preconceptions, issues related to the nature of e-commerce and behaviour. The psychological aspect incorporates the feeling of fear, the need to feel that one’s money is secure, fear from using unknown websites and the ability to control the process of payment and performance of online transactions. There was a widespread perception among customers that e-commerce did not meet these concerns. The following Figure 6.3 shows the category named psychological aspect of security and its
associated concepts, which affect on e-commerce security effectiveness.

![Diagram](image)

Figure 6.3: The psychological aspect of security category that influences on e-commerce security effectiveness

Examples of respondents’ feelings of fear are:

*I fear dealing with unknown websites because there are fake websites that practise fraud. I hear that hackers, who are very clever, steal money and your identity. (Participant 7)*

*Sometimes when I am looking for products on the Internet, I find a webpage with a black background comes up suddenly. This means something to me - horrible and something to do with a hacker, and I wouldn’t buy from this site. On the other hand there are more formal websites, you feel really they’re OK. They have ‘contact us’, this gives you an indication that it’s secure and reliable...but in general the person should be very careful. (Participant 3)*

*The main problem for us is we are not used to using credit cards to buy stuff from the Internet ... but I tried the first time and then I did it again because I had experience, but the first time the fear barrier was with me. (Participant 3)*

*Well, the reason is I have no experience in how to deal with the page that comes up when I select an item for purchasing. (Participant 5)*

Customers had a preconception that buying and selling over the Internet is risky and that this risk is high. Part of this preconception is that the use of e-commerce for buying and selling makes the customer vulnerable and that there is a probability that money will be lost. For example:

*Researcher: Have you purchased anything online?*

*Participant 6: Yes, but I don’t advise you to buy online because it is risky... really hazardous.*

*Researcher: (laughing) Why?*

*Participant 6: I lost money when I tried to do an online transaction.... I did not receive*
the item that I bought... It was about $50.

If I deal with a new website which is not known to me I don't feel confident because I have got a large amount of money in my account. Why should I take risks by myself and lose my money? Here you could lose more than you gain. (Participant 1)

Some websites say '100% secure', but in my opinion you can't believe everything you read. Some of it is rubbish. (Participant 1)

Actually I am reluctant to deal with a website for the first time because I don't want to be a victim. (Participant 1)

Researcher: Suppose you find something that attracts you on an unknown website, do you go ahead with the purchase?
Participant 7: No
Researcher: Even if this website has a good offer, a very cheap product?
Participant 7: Well, you can pay a penny for something but then lose thousands by using a credit card.

I told my bank that I wanted a credit card to use on the Internet, but they advised me not to... because there are many frauds on the Internet, so I changed my mind to avoid any risk... I use it only for shopping from stores. (Participant 12)

The other concern regards the nature of e-commerce, being remote rather than face to face, where the user does not touch or see anything but what is on screen; what lies behind this screen is unknown, which makes users very uncertain.

Researcher: So what do you think—is it secure or not buying online?
Participant 6: It is not secure.
Researcher: Why not?
Participant 6: Because you are dealing with an unreal world, you don't know the identity of the other side, and you just have a screen.

In some cases the expressions of the participants through face to face interaction gave the researcher a real and direct interpretation of body language and feelings, which text does not always sufficiently reflect, with respect to psychological concerns. The above participant’s response can be seen as an example of this situation. [He moved his head and hands, with surprise in his face, signs from him that the Internet is a virtual world where noting can be touched or seen].

The psychological aspect of security also incorporates the behaviour of customers regarding the use of e-commerce. For example, one participant indicated that he was cautious and protected his
passwords from being disclosed, while another saw the following of instructions as sufficient protection.

Well, some of them are secure and some of them are scams, so Internet users should be cautious; for example, many websites send me promotions saying 'Get your gift' such as a mobile or a computer, then it requests your details..... but I don't give them because how can I win something without paying? So these websites lie and just want to get your information.... Personally, I don't open any spam email because I don’t trust it... (Participant 14)

but there are some instructions I should know as a customer to protect myself and my private data.....this requires some caution from me to keep my passwords from being disclosed. (Participant 2)

If they [the website] request unreasonable and unexpected information I don’t deal with them because this makes me suspicious. (Participant 14)

On the other hand, I have two accounts, one with a small amount in, just in case an error happens. (Participant 9)

6.2.5 Cooperative Responsibility

Based on the data, it appears that the responsibility for security awareness is initially undertaken by users themselves and that part of this responsibility is towards the selling company’s website. The user’s responsibility is represented by a continuous process of learning and development of knowledge, which consequently increases awareness; as a result, users can reduce any possible risk they face. Conversely, without this knowledge, customers can increase the risk to themselves. From the next excerpt it can be understood that the user himself has to learn and that this is his responsibility alone.

Why I am learning is because sometimes you have no choice but to buy from the Internet so you need to understand everything relevant. (Participant 9)

The next participant stated that this was his responsibility because he needed to protect himself:

...but there are some instructions I should know as a customer to protect myself and my private data.....this requires some caution from me to keep my passwords from being disclosed. (Participant 2)

The responsibility of all other entities, such as educational organisations (e.g. universities) and the selling company’s own website is to promote customers’ awareness and consciousness regarding the security of e-commerce. For example, one participant pointed out the responsibility
of the education system:

I think [this should happen] through education and this is the government's responsibility. In fact, the government has a significant role to encourage its citizens to use e-commerce as an ordinary thing. (Participant 10)

Some other participants considered the responsibility to be mutual between the user and the e-commerce selling company:

We should recognise that there is a risk. Risk is everywhere, even in traditional shopping. This risk can be reduced and this depends on the user himself. For example, I use a limited card so if I lose money the probability of risk will be very small. On the other hand, the website itself reduces the risk by using better technology to ensure security. (Participant 15)

I think it is the company's responsibility to respect their customers by giving them the information concerning security and telling them how to check the website. But the person himself also has a responsibility – he should learn about everything that's new. (Participant 3)

If the website shows the customer a brief description of what security issues he should be aware of and understand this makes the customer more trusting of the website. (Participant 11)

Thus, customers appear to see the responsibility of companies operating websites as represented by providing descriptions and instructions concerning security, adopting the best technology and providing the required conditions for security. Figure 6.4 represents the category named cooperative responsibility, and the entities (square shapes) involved for undertaking this responsibility, which influences on e-commerce security. While Figure 6.5 shows all categories, were identified from the customer's perspective, which influence on e-commerce security effectiveness.
Figure 6.4: Cooperative responsibility category with the associated entities influence on e-commerce security effectiveness

Figure 6.5: Factors that influence on e-commerce security effectiveness from the customer perspective
6.3 Results of analysis from the organisational perspective

The analysis of data gathered from the organisational perspective, in interviews with managerial and technical personnel, resulted in the identification of seven categories, as described in the following subsections.

6.3.1 The customer’s concerns regarding security and e-commerce from an organisational viewpoint

Some of the respondents gave a general impression of customers’ acceptance of and engagement in e-commerce; for example, one participant believed that customers had a negative attitude to online shopping, marked by a lack of trust and transparency between the customer and the seller:

In fact, from my experience with an e-commerce website for several months, I have come to the unbelievable realisation that Jordanian citizens and Arab customers in general don’t believe or trust online shopping. They think there is no transparency provided by the websites. For example, traditionally, when the customer buys a computer from a shop he faces problems if he wants his computer to be fixed. He will often find that the merchant breaks the contract, and he is always the weakest party so he ultimately carries the cost of fixing the computer. So how do we persuade the customer buying online when he does not see anything with his own eyes and can’t touch it with his hands, when he’s already had to face problems with a physical shop? ... So he needs guarantees.... really, where the detailed information that is provided by the first page of the website is even not sufficient to convince him... briefly, the trust between the customer and merchant is just as poor as it is between Arab customers and their governments. (Business manager)

Another participant, however, was optimistic, referring to the achievements of her company and the degree of acceptance by customers, notably shown by their mature and comfortable attitude to using credit cards.

We adopted an electronic ticketing system on our website, which was an important factor in enabling our business to operate. It became easier for customers to book a ticket and pay online from anywhere... people are accepting ... they are ready, more than you might think, even if there is minor rejection, but in general it was accepted smoothly by our customers...We were really surprised how ready people were to accept that...... The customers nowadays have become used to ATMs. It is not a big deal... most people have credit cards... people are more sophisticated than they were before. (E-business director)

She asserted that they were concerned about customer support, by saying:

The customer viewpoint is considered and we have a customer service centre that is responsible for customers' enquires and claims and problems and we take their
feedback which is important for us. (E-business director)

Another participant who was also hopeful to achieve success, pointed out

*We look forward... Website X will become like Amazon.com... god willing* (Business manager)

Another participant pointed to his company’s concern for the customer in respect of the website design, relating the ease of use of the website with the feeling of security, although he immediately corrected himself, saying that it was not really a matter of security:

*The user’s viewpoint is necessary for us, providing a website that’s easy to deal with, friendly, motivates the customer to use it and this makes him feel it is secure to some extent... not exactly secure.* (IT manager)

The next participant showed how the customer viewpoint is considered and what is done to provide secure online transactions. In his view, it is the simplicity and the truth of transactions with the customer which make him/her feel that the website is secure, which in turn leads customers to continue using the service.

*In fact, the facilities and services that we provide and our security is not just talk, but in fact when a customer enters our website and obtains the product that he wants with the same specifications and this happens easily and without any complexity, this will makes them come again and repeat the experience, because they found that we treated them well. Now we have more than 10,000 active users who buy and sell over our website. Those people, once they have tried and succeeded and found it is secure, then they will become one of our customers and users of our website.... it is just the first trial...* (Business Manager)

He went on to point out that the website also had a forum and rating system, which made the customers feel that the website was credible:

*One of the important things that make the customers feel that our website is secure and credible is the rating system which indicates the positive and negative rankings of the buyers and sellers and the best buyers and sellers... We have a community café on our website and we have seen, for example, one customer ask a question and another customer tells him to refer to our policy, clause number so-and-so. If the customer faces any problem we solve it within 24 hours so the nature of our website is that it’s easy to deal with, so this makes the customers feel happy and confident and in control... it is not complicated.* (Business Manager)

Another participant stated that customer concerns were addressed only through the services provided on the website:

*The customer viewpoint is considered at service level – what he would like to see and*
The organisational contributors did not specify tangible indicators on the website on which customers could rely to check whether the site was secure or not. This is firstly because technical staff appeared to be unconvinced that tangible indicators provide real security: websites are hacked despite the presence of these indicators, so customers could be led into a false sense of security by relying solely on them. Secondly, these indicators assure customers of the organisation’s honesty, for example by using security certificates as an indicator that the website is guaranteed by a third party, and thus that the website is secure, but this provides no assurance that it cannot be breached by hackers.

It is difficult to consider a website secure or not, even if you are professional, no way to say 100% secure, and using a security certificate just means that you are not lying to your customer and are fulfilling your responsibilities, but this is not a guarantee that you are not hacked by hackers. (IT manager)

These indicators (e.g. security certificates) are thus not sufficient to assure users that the website is completely secure. Here the risk does not come from the website itself but from outside parties (e.g. hackers). One participant maintained that there is no way to confirm that a website is secure, even if the website concerned is very well-known:

Frankly, there is no way to judge that a certain website is secure, even if it is Amazon or eBay.... it is reputation and ease of use, the guarantee is experience and reputation. (Business Manager)

A software developer suggested that customers would like to see an electronic receipt, which might make them feel that a website is credible:

Clients may be interested in submitting post messages and receiving email showing their transactions.

Inexperienced customers are also sometimes not aware of technological details, including the meaning of terms like ‘https’. The following are examples of responses indicating that an understanding of security is not important for the customer, whose only concern is the experience of others or the reputation of the website.

Some people don’t care about security – is it secure or not – they’re just concerned about what other people say. If it is a well known company and recommended by other people then they use it and trust it. (IT manager)

To say this website is 100% secure means nothing for the customer. I think the reputation of the website makes the customer feel it is secure. (Support engineer)
The end users don’t know what technology features (security) and applications are used to protect the system. They just need a guarantee that their credit cards won’t be used without their knowledge ... and this at the end of the day depends on the credibility of the company. (Business manager)

The main concern for users is the reputation of the company. They are looking for a well-known company, and people here in Jordan deal with national companies like telecommunications because they know them. (Business manager)

From an organisational perspective, the above quotations show that customers are considered to look for intangible indicators such as reputation, whether a company is well known and the system of rating by previous customers (this point was made with respect to auction websites) for the seller and buyers on certain website when deciding whether to make online purchases. No model is provided for this category where the concepts and meanings presented in the above quotes are implicitly covered in other categories.

6.3.2 Psychological aspect of security

The organisational contributors also reported a belief that customers can be seen to have fears and feel that e-commerce is not a secure channel through which to buy and sell over the Internet; in other words, they have a negative preconception of e-commerce, involving undue risk. The following figure shows the category and the concepts being the same as were presented in Section 6.2.4 with regards to the psychological state of security from the customer’s perspective.

![Psychological aspect of security](image)

Figure 6.6: The psychological aspect of security category that influences on e-commerce security effectiveness

The following are examples of organisational participants who reported that people were afraid
to use credit cards for buying online:

In Jordan it is difficult to say that there is real e-commerce ... I mean the percentage of people who use credit cards to purchase over the Internet is very low and only a few people do, because ... the notion of using credit cards online is still not acceptable. They fear, they don't trust the machine. (Support engineer)

... there's a percentage of people who are afraid of using credit cards over the Internet, so those people won't give their card details over the Internet. The second class [of people] are those who don't want to learn and discover what is new, so they are still afraid of ... buying online. (Business Manager)

Another participant, while agreeing, felt the younger generation to be more knowledgeable:

I mean the former generation is afraid but the new one is fearless and more practical, so they use the Internet to buy and sell and browse and search and share and everything. (Customer support)

Some participants addressed the issue of the nature of e-commerce mentioned in Section 6.2.4:

To be frank with you, people still have fears... you interact with a product or service that's intangible on your computer screen. This is not only true in Jordan but in all Arab countries. In reality there is nothing between your fingertips. (Business Manager)

Customers are afraid to buy online because it is not face to face and those who buy online use only trusted websites. (Support engineer)

They highlighted a perceived difference in mentality and beliefs between people in Jordan and those in other parts of the world:

The nature of people here in Jordan and their mentality is different from those from Europe and USA but nowadays there is the CashU card which is limited and you can use it to purchase online and with low risk. So if he wants to worry he will only worry about $30. (Support engineer)

People still have beliefs that doing online transactions is risky and they are afraid, so we need to spread consciousness in society. (Business Manager)

6.3.3 Users' characteristics

The organisational perspective also reveals users have varying levels of security awareness characterised as professional, courageous, ignorant, afraid, and new generation users. These attributes can be seen to be closely related to users' experience, knowledge and willingness to experiment, as mentioned in Section 6.2.1. They were depicted in Figure 6.7.
Learning nowtedge ý''ýexperimentation expenencý user characteristics Influence on E-commerce Security Effectiveness

Figure 6.7: User characteristics category influences on e-commerce security effectiveness

It can be said that those users who are familiar with security features on e-commerce websites and have the ability to differentiate between genuine and fake ones, feel confident enough to perform online transactions. Some users’ initial experiments with such transactions determine whether they decide to repeat them or not, as reported previously under the customers’ responses in Section 6.2.1. Some organisational participants stated that:

*Some of the users have the courage to experiment and this will in time increase the acceptance of e-commerce.* (Business Manager)

*People start feeling comfortable after the first experiment and see how it is secure and saves the individual’s time.* (Software developer)

Other users try to understand what they need to know in order to perform their transactions securely. This type of user may be stimulated by other people or simply be curious. Some users do not own credit cards and see e-commerce as posing a great risk of financial loss. One participant classified users based on their experience of websites:

*There are two types of people. The first type is professionals and has excellent information and confidence in buying via the Internet and the second type had less information and these are in two groups. The first group want to develop themselves in line with the technology, to examine and experiment and learn from other users, friends, who have tried before. Besides their courage, some of these users are curious to discover new things. The second group don’t want to learn and discover what is new, so they are still afraid to use the Internet for buying online.* (Business Manager)

The same participant asserted that people in Jordan are knowledgeable:

*There is a street in Jordan with a record number of Internet cafés (in Guinness Book), which means large Internet use... this means that people have the knowledge and skills to deal with the Internet.*
The data revealed a perception that there are also users looking for new or easy functionality or to gain prestige through utilising technological developments. All of these types represent the new generation of users; the older generation meanwhile fears these new developments because they do not feel in control of a situation in which they are buying online.

..but the new generation of youth who are educated are open-minded, looking for everything new, and easily accept the technology. This generation is more flexible than the last one. My son is 12 years old and uses mobiles, computers and the Internet easily. When I compare this with my era there really is a big difference. (Customer Support)

...the new generation is aware of the new technology and they keep up to date with new fashions. (Engineer support)

6.3.4 Social communication

Social communication is a means of broadcasting awareness and perception of security issues. It includes talks, beliefs, stories, and experience that are shared between individuals and groups with respect to e-commerce specially and IT usage in general. Figure 6.8 depicts the social communication category and its related concepts, which were extracted from the following excerpts.

Users appear to be affected by a set of shared values regarding the use of e-commerce and its security. This was reported from the organisational perspective as well as the described customer responses in Section 6.2. For example, one organisational staff member said:
We have a community café on our website and we have seen, for example, one customer ask a question and another customer tells him to refer to our policy, clause number so-and-so... (Business Manager)

Social communication consists of others’ experiences, reports of past successes and failures, by word of mouth and via the media, as was stated by some participants from organisation:

Some people don’t care about security—is it secure or not? They’re just concerned with what other people say. If it is a well known company and credible according to other people, then they use it and trust it. (IT Manager)

People use websites that were used previously by other people. (Business Manager)

If users see that others are confidently using a certain website, they will tend to follow suit, irrespective of their own experiences of the security features on that website. In fact, this was stated by one customer:

I heard that a padlock at the bottom of the page means that a site is secure, but I can’t tell you if it is actually secure or not, but the main thing for me is what other people say, because they have more experience of these sites than me.

In addition, word of mouth can work both negatively and positively. A person telling a friend of a bad experience with a certain website in which they lost money will tend to put that friend off. Likewise, a bad initial experience with e-commerce will tend to discourage some people completely, as stated by a customer who reported a negative experience:

I don’t advise you to buy online because it is risky...

One organisational participant referred to this phenomenon:

One of the key points in Jordan is word of mouth ... my friend says that... my friend has experience ... next day he goes and tries the same website because it was trusted by others. (Support engineer)

In essence, social communication affects the construction of the mentality and behaviour of individuals regarding the use of e-commerce and its security. Media-based marketing, especially via local media, also has a certain status that will lend credibility to websites advertised through such means. The media (i.e. newspapers, TV, Internet and radio) can contribute to disseminating positive attitudes and to reducing the spread of negative ones regarding the use of e-commerce and its security. For example, one participant from organisation said:

The media has an important role in raising public consciousness via radio and TV to encourage people to use credit cards and to use certain websites to buy and sell...
online... all of us listen to the radio, especially in the morning when we are driving to work. Why don't we utilise it...? (Customer support)

6.3.5 Management commitment

Organisational participants indicated that the commitment of management was expressed through expenditure on security and support technology: they felt that higher management had a responsibility to adopt such expenditure as policy. For many reasons, including competition, businesses consider that expenditure in security should be seen as making a profit, because they help to expand the company's work and strengthen its reputation. For example, one participant offered this view:

Let me tell you something important. If a business wants to survive and continue to compete it needs to be mature enough, the aware company realises that it is normal, even if it adds cost, for security insurance and this should not be seen as cost but rather as profit and as increasing their income, even though this will take a long time.

(e-Business director)

She stated how the top management provides unlimited support:

Actually, our success comes from our management commitment. They are very serious and their support is tremendous. Each month we discuss our achievements and review our work. They give us unlimited support, financial and non-financial.

She continued:

We pay millions for our systems... we have a rule that investing in technology is important for survival, otherwise you will die.

Such considerations serve not only to increase a company's standing with customers, but also to forestall potential disasters by ensuring a solid database, including sensitive information and financial data, on the website's back end, with mechanisms to prevent unauthorised access and modification. A security manager stated:

Security is essential in order to protect you before protecting your customers, even if it is costly.

Another issue, which is part of management role, emerged from this discussion is that some businesses buy systems from IT providers rather than developing them in-house. In essence, such businesses have an outsourcing strategy:

Let me tell you the truth now: the world is moving towards outsourcing because it is cheaper and quicker than building systems in-house and at the same time you are buying from well-known IT vendors. (E-business director)

109
If the outsourcing strategy is adopted, then as reported by one organisational staff, the company determines its business requirements, including security requirements, invites tenders from potential providers, and then evaluates their proposals. For example, in selecting the best provider for its Electronic Payment Gateway (EPG), a company has to assess the distinctive attributes of each, such as ease of use, as well as considering the assessment and feedback provided by other businesses regarding the security of each payment gateway. Thus, one participant said:

Another point is that businesses can give feedback and assurances to other businesses that this electronic payment gateway provided by X is secure, and they can refer to them and ask them if they faced any problems and if they were solved or not. (Business Manager)

Management's vision should be open-minded and encourage continuous development of technology, as well as supporting the improvement of technical staff skills through training in order to keep their technical knowledge updated, especially with respect to security issues.

Our management is open-minded ... most of them have studied outside Jordan, in the UK and the USA, so they benefit from outside experience and can utilize it in Jordan. (Support engineer)

The IT people should also be supported by the management.... they should send them to participate in courses and training, especially in security, in order to develop their skills. (Security manager)

In our company we always move as the technology advances and follow developments in tools and languages and by considering security features. (IT manager)

The following participant pointed out that Jordan has qualified IT personnel who have developed a national secure EPS project, which links e-service websites from outside Jordan:

The whole project was developed in Jordan .... We have skilled IT staff and competencies.... We did not face any technical difficulties. In fact, we exported the project outside Jordan to Dubai and Saudi Arabia. We host governmental institutions and provide online payment facilities. (IT manager)

One participant revealed how his top management provided individual reward:

I want to give you an example of how our management supports us, even individually, and how they reward us based on our achievements.... You see this watch? It is worth about $.... They pay us well for our efforts. (E-business director)
There is also a need for policies to protect systems and servers from problems, and consequently for environmental and physical security if required in the context of security implementation, as well as clear policies for customer support.

*Frankly, the presence of the policy is necessary, and this policy should be supported by the higher management, otherwise you can’t do anything in order to protect the system and data, and there should be procedures for applying the policy and making evaluation frequently in order to identify the weak points and strengths.* (Security manager)

One participant pointed out the importance of the role played by business managers and their awareness of the need for enhancing the security of the website, emphasizing how this lack of awareness is related to costs reducing:

*Some websites in order to reduce expenditure do not get a security certificate from VeriSign, just to save $500. This is a question of business awareness... They do not know that this certificate supports their business and makes the customer trust them.* (IT manager)

The same participant pointed out how the managers of banks are reluctant to make decisions on providing cards for online payment:

*We started with one bank which authorised its cards for use online and the others waited to see the adoption ratio... what happened with the other bank ..... Then the others followed the first one, gradually the 10 banks in Jordan will be connected by PayOne [electronic payment gateway] and provide cards for online payment.*

Another participant showed how the staff and top management work to support customers:

*Support and business management staff meets regularly to cover problems with customers. We work together to make improvements for customers and if there's any feature we think we could provide on the website, we set up 100 scenarios of what will happen with users if they use this feature. We work for the customer's support and comfort.* (Business Manager)

According to the above quotes revealed by the participants the following figure depicts the management commitment category and its associated concepts.
6.3.6 Implementation concerns

This category comprises four further subcategories: e-commerce and security infrastructure, security tools, security practices, and security during the process of e-commerce system development. These were depicted in Figure 6.10.

1. E-commerce and security infrastructure

The data shows that the main component of full e-commerce is the EPS, also called EPG; the participants referred to the associated problem that in Jordan there is no national EPS, which also involves security insurance, as it includes the processing of financial transactions. For example, a business manager said:
Do you know there is still no Arabic electronic payment gateway? And as you are aware it is difficult trading electronically without one. To explain the idea, as I conduct business online I have to provide payment services on my website by credit cards—Visa and MasterCard—but in order to do that you have to connect your website with an electronic payment gateway that provides you with security over the Internet. Here you have to open a merchant account in the USA and then enter a thorny process.... your money will be transferred to your account after deduction of the commission for each transaction by the provider. To some degree you find it is not profitable, in fact in some cases you pay fees even though no transaction has taken place through your website.

Another participant made the same point with respect to the lack of an EPS in Jordan:

One of the challenges we have faced is providing an electronic payment gateway ... we should provide our customers with a secure payment gateway. This web service – we got it from US company. In fact, there are only one or two companies in Jordan but they are not strong like these from outside, as our business means you have to deal with international firms and secure and well-known ones which are accepted by everyone. This is because our customers are not only from Jordan but from outside, so we need something known to all people. ... when we decided to add this facility we evaluated many companies that provide EPS and chose a popular one that uses plenty of security checks. (e-business director)

This participant also referred to the familiarity of the EPS provider and noted that the criteria for selecting an EPS provider include popularity, reputation and security concerns. It also depends on the nature of the business; some trade requires the presence on the website of an international EPS which is known to people all over the world (e.g. a website for booking tickets).

Another participant pointed out that the number of business websites in Jordan providing full e-commerce, including an electronic payment service, is very low:

There are few websites that cover full e-commerce solutions such as e-payment services like that offered by Orange and Umniah .... In reality, e-payment technology is used in only a few cases ...but this [presence of EPS] encourages people to take the risk of paying their mobile phone bills online. These projects are increasingly widespread in the Jordanian market and e-commerce will be the primary requirement for all enterprises in the future. (Software Developer)

The availability of EPS is essential in order to perform any online transaction, which entails security insurance to ensure that data is encrypted and protected before the financial transaction proceeds. Without these measures, the interviewees indicated that there can be no full e-commerce, only electronic marketing.
Well, if you are talking about purchasing and paying over the Internet then we should talk about the availability of electronic payment systems, but if you are talking about normal websites just for promotions, then it is not necessary to talk about security. Actually, the issue of EPG is still a problem for business in Jordan. For example, I know one online auction website in Jordan was closed because of the problem of adding this service to their website. They found it cost them more than they expected so how could they have a secure process of payment with no independent financial institution to undertake this activity? (Business Manager)

This means that companies that intend to do business online could fail for lack of a secure EPS. Thus, the availability of EPS enables businesses to support their transactions and so to add e-payment services to those available via their websites.

The following participant pointed to the security solutions that are considered in the new developed national EPS:

All banks register their cards by VbV [Verified by Visa] 3D secure protocol. The general idea of VbV 3D secure is to enhance security for using cards online by ... verifying that the person who uses the credit card is the person who is eligible to use the card and no one else, by prompting the user to enter a PIN or password as well as the credit card information – and this helps to reduce cases of fraud.

He went on to list the security standards that are applied to provide secure EPS in e-commerce:

Everything standard is applied in our EPG... SSL, no data stored in the merchant, PKI, hashing.... We use signed applets ...Java is applied to prevent hacking into the code... we use PCI compliance [Payment Card Industry Data Security Standard.] (IT Manager)

PCI is a standard used for enhancing online payment data security, including details about security requirements, polices, procedures and security of the network.

Another issue related to the international EPS is that even the providers (e.g. PayPal) are well-known internationally and are very secure, but the problem here is that some complicated procedures and many documents are required by the provider; for example, one interviewee said that one EPS cannot be used to make donations, while another requests a guarantor.

We ask our clients which electronic payment gateway they prefer and we ask about the nature of the product they want to offer via the website, because some electronic payment gateway providers do not accept the payment of donations, an example. ...some international payment gateways request many documents and their procedures are complicated. (Support engineer)

The other factor is that some EPSs, in particular their interfaces, are difficult to deal with. Once
users transfer from the e-commerce website layout to the EPS layout, they are faced with different styles and designs that cause problems and confuse them, making them feel that they have lost control of the transaction. As the following participant said:

The choice of payment gateway is very important since the customer wants to interact with an easy and friendly interface without any complexity, but some of them confuse the customer when he moves from the design of the company website to the EPG provider design and some of them require you to register before you proceed with the transaction. (Support engineer)

The e-commerce websites launched from Jordan mostly depend on external EPS providers such as PayPal and 2Checkout to provide the facility for electronic payments. For this reason, one interviewee indicated, for example, that if EPSs were run by nationally known providers, they would be better accepted. This means that not all customers and Internet users know the international EPSs, which is one reason why the absence of secure EPSs in Jordan restricts the acceptance and success of e-commerce. The participant said:

We offer our clients the 2Checkout and PayPal services because they have good reputations, but frankly these international ones don't make online purchasing a national phenomenon at country level. But a payment gateway provided by the government would be used for public and national purchasing because not all people know these international companies. Besides, they trust the government to do everything to protect the customer and serve the public interest. (IT manager)

This participant stated that the reason for choosing international EPSs was their good reputations. Nevertheless, he suggested developing a national secure EPG supported by the e-government project to provide payment by different methods through electronic bank accounts or credit cards. This would enable businesses in Jordan to use an EPS on their websites as an interface similar to that provided by the e-government portal, consequently enabling them to engage effectively in e-commerce, performing electronic transactions securely and at low cost. On the other hand, it would also increase the level of acceptance by customers. Citizens would accept an EPS provided by the government because of the general culture of reliable provision of most public services. Payment on certain websites via national secure government payment gateways is secure and guaranteed. This also indicates that the success of e-commerce in Jordan is correlated with the success of e-government. The following excerpts confirm this:

I think the availability of a secure payment gateway via e-government would enable businesses and customers equally to enter any website and perform online transactions ... buying and selling spontaneously and paying by credit card or bank account so any e-commerce website would direct you to the e-government payment gateway...... The
use of e-commerce would be doubled if there were a secure government electronic payment gateway.... otherwise e-commerce will not develop and advance. (IT manager)

It can be said that there is a significant relation between the success of e-commerce and e-government, as stated by another organisational participant:

*We told the government if it wants e-commerce to succeed then it is not acceptable to perform transactions in the traditional way... the government should move... we will sign a contract with the government to provide her the EPS for all its departments. (IT manager)*

The enforcement also appears here where any revolution or new technology imposed by the government leads people to conform to it by trying to understand its characteristics. It is debatable which of e-commerce or e-government comes first. Whilst it is known that the term 'e-commerce' was coined first, the acceptance of people dealing easily and comfortably with e-government services may encourage a popular engagement with e-commerce, especially when payments on e-commerce websites occur via secure e-government payment gateways.

The participant who suggested developing a national EPS via government support continued by stating the advantages of this course of action:

*This would also give businesses in Jordan ability to integrate this web service into their websites, where the same electronic payment gateway that is used in e-government websites would be used by business, as a result gaining the favour and approval of customers, convincing them that it was a secure way to pay online, since everything provided by the government can be guaranteed. As a result, this would reduce business costs compared with using international overseas electronic payment gateways which are not accepted or known by customers. (IT manager)*

The newly developed national EPS provider claimed that the fixed cost per transaction was less than other for international EPS providers:

*The merchant pays only a one-off payment of 350 JD and we take commission of 4% for each transaction... This is less than paypal, which takes 5%... if the merchant does many transactions per day and no fraud cases arise, then we reduce it to 3%. (IT manager)*

The national EPS provider also referred to the technology used for developing the EPS, which is compatible and thus suitable and interoperable for integration with the two most familiar development environments:
2. Security tools

The respondents referred to groups of tools that can be used to enhance security. Tools should be configured in appropriate ways, because default settings are known to be susceptible to hackers. These tools vary in the level of use; examples are tools such as ASP.net and JSP concerning programming languages. These tools have some features supportive of security. Tools at network level include intrusion detection systems, firewalls and the use of server features. Tools supported by Internet browsers include Secure Socket Layer (SSL) protocols. Tools need to be changed in response to technological change. For example, one participant said:

*In our company we always move as the technology advances and develops in tools and languages, and by considering the security features.* (IT manager)

The researcher looked for multiple evidence of the same concept; as an example the above participant continued by saying:

*All pages of our website have https secure contents which use SSL, while the pages that do not request sensitive data are normally http pages.* (IT manager, website)

The researcher therefore went to the website and examined its features to confirm this. Another contributor said:

*We plug the project with an SSL certificate. For example, we once used an SGC (Server Gated Cryptography) certificate with EV (Extended Validation) supplied by VeriSign.* (Software developer)

Other participants referred to the environment in which their websites were developed:

*We use security at tool level provided by Linux and SQL. Security is a high priority for us – security of the database and security on the JavaScript pages.* (IT manager)

*There is a feature in ASP.NET 2.0 which hides HTML source code in the web page.* (Software developer)

The Security Manager reported that total security was not provided by the third party, namely the EPG provider:

*The security does not only depend on the EPS provider, because security breaches could occur on your server.* (Security Manager)

He added, in regard to the security of servers:
Security should apply to data in company back-end databases, so no one can access these data, only the legitimate employees. On the customer side the website should also restrict the access given to users and what services they can access; otherwise, if a customer can do what is not permitted for him, then there will be an error in the E-commerce system. Some companies set a server as a mediator register or as a log of customer transactions before access to the back-end database besides using a firewall... and an intrusion deduction system which work like a monitor. This software and hardware should have the correct ... settings, because there are default settings which are known to hackers, so they are easy to breach, so these settings are needed to ensure security... If it is left at the default setting as provided by the company then there is no security. (Security Manager)

Using more than one server provides additional security, as end users have no direct access to the database. (Security Manager)

Another participant said that facilities were provided by certain server types:

Security procedures are offered by the web application server... In the case of the Tomcat web server, there are many security facilities such as allow/deny directory access, access control on your server, user authentication ... installing a firewall such as ISA (Internet Security Accelerator), installing antivirus software... (software developer)

The next two participants referred to the security standards that are applied to e-commerce applications and which are common to all known websites:

Everything standard is applied in our EPG... SSL, no data stored in the merchant, PKI, hashing.... We use signed applets ...Java is applied to prevent hacking into the code.... we use PCI compliance. (IT Manager)

What do you want?... Everything that is applied to the best-known websites in the world is available on our website. (Business Manager)

This means that the problem is not in security itself (i.e. the product), but in undertaking the responsibility of providing security, which involves awareness on the part of the higher management, applying the standards responsibly, spending on security and raising awareness among customers of these standards; or at least the perception that the companies have applied the relevant security standards to their websites, which makes people more confident about transacting online.
3. Security practices

Security practices represent the procedures that are followed by IT staff in order to guarantee and enhance the security of e-commerce websites. The following are sets of practices that emerged from the data.

- Provision of data; frequent back up in case the database is lost or the server goes down.

  *The log file gives you all transactions on the system... and the deduction system can tell you if breaches have happened... Making frequent backups of your database will protect you if something unexpected happens.* (Security manager)

- Identifying access privileges for each function and service on the website.

- Disabling of the “back” button after logout:

  *The webpage that allows the customer to log in to his account must prevent the customer from returning after he has logged out. Another example of security on the website is allowing the user to enter his username and password 3 or 4 times, after which his account should be locked (e.g. bank), and if he logs on he should have limited privileges and services.* (Security manager)

- Ensuring that website interfaces handle data correctly without faults and errors, which could cause security breaches and create opportunities for hackers.

- Visibility of the logout icon.

  *The interface should request correct data from the customer and ensure that only the correct entry is made to avoid any possible errors. It should reject disallowed characters which might be used for database injection... the input data is specified based on the specifications of the system. The webpage should include a logout icon in order to enable the user to quit. This icon should be set in a clear place.* (Software developer)

An participant pointed out that

*Sensitive parameters should not be passed in client query URL parameters but through hidden form parameters.* (Software developer)

- Enhancing the password system
  - Use, for example, a minimum of eight characters
  - No repetition
  - Forcing password changes
  - Enabling password changes
  - Lock access in case of incorrect password entry
  - Remove tick defaults
  - Token passwords.
For example, one developer said:

A simple thing that might cause an error by the programmer is when he keeps the password as “remember my password” ... therefore the password is stored on the computer, then any one who enters can use the previous account; the first user didn’t see the small tick in the box so here the identity is used by someone else. (Software developer)

In addition, the password should be mentioned in the policy:

The password system should be mentioned in the policy and should be strong; it should state that the user’s password must be changed every 6 months for security reasons, use of similar characters should not be allowed, and at least 8 characters, as an example. (Security manager)

He continued:

On the other hand, the password alone sometimes is not enough. We need something else to ensure the authentication of the user and this information is taken via telephone, beside using a token which is changed every time you enter the online bank. But if a user trusts a friend and gives him his password and token, then it is his responsibility if any changes happen in his account.

- Developing security resolution centers in the website for solving user’s problems; these provide customers with answers to any queries and problems, demonstrating that all difficulties have been anticipated:

  We have a security resolution centre, where any customer who has problems just has to specify the nature of the problem and within 24 hours we will try to solve it. For instance, if an item is not received, is not the same as what was ordered... We mention most of these problems on the website and the solutions to them. Once the customer sees we cover all these problems and we have considered them then he will trust us absolutely and feel that our website is secure. (Business Manager, website)

Such problems might be related to physical issues, where the delivered product is not the same as what was ordered; the above participant continued by saying:

  In our security resolution centre, over the website, we receive many reports of problems from customers; for example, one says ‘I did not receive the item’, while another claims that the item is not the right one, so we try to keep in contact with them and solve their problems.

- Developing a library of security breaches which records such breaches and how they were solved, giving the programmer a basis for solving future breaches.

- Session timeout:

  If the user has logged onto the website through his username and password, the website should disable any new session with the same username and password.
All sensitive pages include https:

All pages in our site use https secure page contents, which uses SSL. (IT Manager)

Provision of conditions for the protection of systems, servers and hardware (environmental and physical security):

There are three types of security in general. Physical security: the location of computers and servers; environmental security: protection from earthquake and fire; and logical: specifying the user's access and interaction with the system. Of course a policy ... should be set up for dealing with each type. (Security Manager)

Providing security policies on the website, as one participant stated:

Besides, our policy stated on the website is very clear and specifies our liability. (E-business director)

The researcher examined the security policy as stated on the website of this company:

We will take appropriate steps to protect the personal information you share with us. We have implemented technology and security features to safeguard the privacy of your personal information. (Website X)

The security policy of the second website company was shown to the researcher by the business administrator:

[Website Y] takes every precaution to protect our users' information. When our registration form asks users to enter sensitive information (such as credit card number or bank details), that information is encrypted and is protected with the best encryption software in the industry. (Website Y)

These two security policies give the customer a feeling of the credibility of the websites, as both claim that the best security and technical features are employed.

4. Security during e-commerce system development

Security controls or checklists are not added after the e-commerce system is built, because, as security manager explained, some faults and errors could occur and then the system would be able to be breached, which would require time to be spent in retesting the code, fixing the errors and checking the security requirements. Many such corrections would involve the programmers having to rebuild the system from the beginning, consequently wasting time and money. The development of secure e-commerce websites therefore involves a security auditor or team from...
the outset. For example, one security manager explained the reason for addressing security issues at the outset:

> At the beginning of system development the security manager or auditor should be involved ... they are responsible for early security checks ... If these checks are done after the system is finished then more time will be needed and it will require a lot of fixing. Sometimes you reach a stage where the system has to be rebuilt from scratch and this is really difficult. The elements of the e-commerce system must be coherent and integrated in order to be secure. (Security manager)

In addition, this security manager indicated the necessity of involving the security auditor with other personnel responsible for the development. The security team identifies the security functions with reference to the customer, and they consider even those that the customer has not specified explicitly, because without security the system is not workable.

> Any website where there is interaction between the customer and the website must provide sufficient security. Some of our customers request security if the website involves paying online by credit card and some customers (business clients) don't ask about that, but this our responsibility even though the customer did not request it. (Support engineer)

> Security is a functional requirement .... Any system without security is partial and not complete, especially if financial matters are involved. Security is essential in order to protect you before protecting your customer, even if it is costly. (Security manager)

The security function is considered from beginning to the end of the traditional process of system development. At the requirement analysis stage, the security requirements are considered by defining what functions the e-commerce system should and should not perform; at this stage security requirements are considered as essentials, these requirements being collected from the customer (i.e. the company). One of the participants asserted that

> We consider the security from the beginning stage because it is a core function of any e-commerce system.

He continued:

> In general, the security requirements tell you what should be done and what shouldn’t be done and this is specified by the system requirements when we collect them from the customer... we model the security functions, for example the login function, by using use case/class diagrams and we draw several scenarios: if this action is done what will happen and if it is not done what will happen? (Software developer)
In essence, it is important to model the security functions to show the actions/interactions and flow of data between website functions. For example, authentication is an essential security function which should be modelled for example by a use case/class diagram that shows the login on the webpage: if the username and the password/PIN are identical with those stored in the database, the customer is allowed to enter his/her profile in order to perform the transaction.

In regard to the implementation stage of e-commerce systems, tools and practices, as mentioned in previous sections, are taken into account to see if any need to be used, configured and applied to enhance security. Finally, testing is done function by function as one of participants suggested, in order to ensure that each is working well, until the whole e-commerce website becomes workable. Testing is important to ensure that the system works perfectly. Security auditors could also test the system by acting as hackers, as reported by one participant, in order to determine whether or not the website can be breached.

The security manager or auditor should work as a hacker trying to breach the system, not just ensuring the correctness of the entered data ... he should test what will happen if he enters incorrect data, since that is where breaches come from. There are some companies which specialise in checking systems to see if they are secure or not. They try to breach them in order to test them. (Security manager)

Some companies depend on an outsourcing strategy and have no involvement in the process of development; their responsibility is just to integrate their e-commerce website with the services provided:

Nowadays, the trend is to buy the system from an IT provider and just do the integration. You make an interface between your website and the web service and usually the IT vendor company uses a known programming language in order to be able to find support from the company itself. This approach is better than if you develop the system in-house. (Security manager)

Another participant reported that although his company depended on outsourcing, it had skilled staff:

Even though we outsourced our system we have a technical team who are specialised and skilled. They specify the system requirements and integrate our systems together. (E-business director)

The next participant indicated that the IT provider undertook to provide a secure system or service, once the company had specified its security and business requirements:

In fact, we outsource our systems from an IT provider, so they take charge of providing
us reliable and 100% secure systems. We prepare our invitation to tender where we specify our system requirements (business and technical requirements), including of course security, and this is the standard which is used in all popular websites ... we use it (encryption) as in Amazon. And let me tell you the truth now: the world is moving towards outsourcing because it is cheaper and quicker than building systems in-house and at the same time you are buying from well-known IT vendors. (E-business director)

6.3.7 Cooperative Responsibility

The organisational staff made reference to the contributions to e-commerce security required by both the public and private sectors. The responsibilities here are cooperative. In order to delimit these responsibilities, it is necessary to identify their parent entities and the role allocated to each. These entities, as mentioned in the data, are the public sector, private sector, government, universities, media, banks, users, e-commerce websites and business personnel, including IT managers, security auditors and higher management. Figure 6.11 depicts the category: cooperative responsibility as a central factor linked with other categories. As shown in the figure, there is a mutual responsibility by the government, banks, universities, the organization owning of e-commerce website and the customer via the social communication (formal and informal). There is also cooperative responsibility by the government, banks and universities toward the implementation concerns, and there is responsibility by the organization’ management. The above mentioned entities are part of the responsibility and complement to each other.
The government, by providing a secure national EPG which gives companies the ability to execute their business securely through it, as well as making them cost-effective, thereby encourages businesses to engage in e-commerce.

_The use of a secure electronic government payment gateway increases the usability and diffusion of e-commerce in Jordan and consequently this will not succeed unless the government supports it. (IT manager)_

Another participant suggested that the government should introduce initiatives to increase the adoption of e-commerce:

_We told the minister if there is no initiative for e-commerce we will develop EPG and provide shopping commerce, even though that is not our role, because we are a facilitator between the banks and the merchants. (IT manager)_

He continued:

_We told the government: ‘If you want e-commerce success then it is not acceptable to perform the transactions in a traditional way…’ The government should move…_

It is the education system’s responsibility to increase individual awareness and perception, enriching knowledge and experience of the security and use of e-commerce, as well as
propagating a culture of using e-services to carry out activities on the Internet. Universities and schools perform this function for end users and technicians alike. Education programmes teaching e-commerce and information security ensure the practice of these disciplines in real life, both by technical staff, who can develop secure e-commerce websites, and by general users, who are encouraged to use e-services with confidence.

I think this can be done through education at universities by providing courses specialised in e-commerce and IT security, and these should be generalised to all universities, but ... the new generation accepts this easily and it is more modern. (Customer support)

I would say that government support also has a necessary role and we have to think about that like any project at the national level. And his Majesty is determined to succeed in e-commerce and IT generally in Jordan. In addition, the consciousness among business communities is important. (IT Manager)

You don’t know how far the new generation is educated - in private schools the students are learning how to design websites....(e-business director).

I think education has an influence (Business Manager)

The government has the biggest role ...through the universities and schools ... the new generation are more aware ... the older generation will never change...

The banks also have an important role in providing customer facilities for credit/debit cards and in issuing cards for limited amounts, enabling customers to use them for shopping online, thus reducing the level of potential risk. They are also responsible for coordination with other entities.

In addition the bank has an important role to provide customers with limited cards for small amounts like $300 so this reduces the risk; therefore the assistance should be provided by banks as well. (Business Manager)

There is a communication link between the education system and banks. The banks provide facilities for the users of credit cards. (IT Manager)

Another problem is related to the banks’ present procedures, where their cards can be used to buy online only if customers request this facility, as a participant pointed out:

In Jordan, there are about 1.5 million credit and debit cards, but the default is that these cards are not accepted in online sales unless you ask your bank to add this service....otherwise the card is rejected for payment online. (IT Manager)

The participant added more details on this matter:
Banks in Jordan only allow cards to be used for purchasing online based on a request from the customer.... Banks do not provide this service for all cards because they pay fees to Jordan Visa for each card, so they just provide it based on request... it is free for customers..... Now we propose a model for registration of all cards to buy online, but the fees are deducted from the banks by Visa if the customer wants to buy ...the problem here is that the customer must register if he wants to use it online.... This could cause confusion for the customer and here the bank has to tell the customer: 'If you want to use the card online you have to register online first' ....the popup window on the Visa page might worry him... the easiest scenario is that the bank takes this step, not the customer... (IT Manager)

The role of banks is also considered by the same participant, who addressed the problem of cooperation by the banks in respect of developing a national secure EPS, as well as considering the government’s role:

we face a cooperation problem with the banks ... they give us low priority... work that could be done within two weeks takes 6 months. It takes a long time to connect the server..... We did not face any technical difficulties; rather we exported the project from Jordan to Dubai and Saudi Arabia and other places. We host governmental institutions and provide online payment, whereas our government still does nothing .....We were ready but the government moves so slowly... (IT Manager)

Businesses engaging in e-commerce have a responsibility to develop secure websites. They exercise this responsibility through their sites’ security features, the security materials published on the sites, and by providing brief security explanations and checklists of important security points. Part of this responsibility lies in a management commitment to the necessary expenditure on security, as mentioned in the previous section.

Now many websites provide clarity for the customer in detailed step by step instructions on how transactions take place and what he needs to check in order to complete his transaction securely (Business Manager).

This participant added:

We have made our website 100% secure. We carry the responsibility for that. There are websites claiming to be 100% secure, but they are not secure, just talking rubbish. In our website also we give the customer an explanation regarding the security and the privacy policy, also we provide a service on our website which is a community for our customers. They enter and discuss issues regarding the websites and its facilities and the problems faced by customers.

In this regard, the researcher examined the website in question, which clearly displays logos that are there to inform the customer on issues related to security and to make him feel that the
website is secure. This also shows the website provider’s responsibilities. The following logos were found:

100% Secure Trading

Customers are also advised to check the padlock, as indicated by the following reminders:

- Look for items with this icon.
- This means that the auctions displaying it are more secure.
- Dealing through [website X] guarantees 100% secure transactions.

Other examples show the responsibility of the company management for expenditure on security and protecting the customer’s data:

- Let me tell you something important. If a business wants to survive and continue to compete it needs to be mature enough, the aware company realises that it is normal, even if it adds cost, for security insurance and this should not be seen as cost but rather as profit and as increasing their income, even though this will take a long time...
  (e-business director)

- Security depends on the responsibility of the website company because if the website uses the best technology to encrypt the data and no one can decrypt the data through transmission and the website guarantees that... but once this data is in the hands of the website company and it then distributes your information to other websites, then it is not secure. (Security Manager)

The EPS developer said that the responsibility of providing security advice and instructions to customer is not theirs; rather it is the merchant’s responsibility. When the researcher asked the EPS developer whether the EPS interface provided security advice for the customer, he replied:

- In our package we do not provide any advice for customers about security ..... I think it is the merchant’s responsibility, not ours ... Maybe both... maybe we should inform the customer about security checks. (IT Manager)

Websites that present such information to their users so that they can verify before conducting their transactions encourage them to feel that they are committed to their customers’ security. In
essence, part of the company's responsibility is to protect its customers' data, as shown by the above quotation. Websites should provide customer service support and security resolution centres to solve problems faced by customers. Such facilities are set up by technicians with the responsibility of developing secure e-commerce websites by considering all the concerns regarding implementation that have been discussed in Section 6.2.6.

The responsibility of the media is to promote and market via TV, Internet, radio and newspapers a positive view of the use of e-commerce, especially of major commercial and national websites.

_The media has an important role in raising public consciousness via radio and TV to encourage people to use credit cards and to use certain websites to buy and sell online... (Customer support)_

_We have a media role to educate people and encourage them to purchase from the Internet. On the other hand we need national statistics showing numbers of e-commerce transactions and the number and amount of payments, and this requires cooperation by the public and private sectors in order to reach the desired goal. The role of statistics is that it shows us where we are now and where we will be, and when, so that we can build on it. (IT manager)_

_The attempts by physical companies to increase their sales and promote their businesses use promotional strategies to tell people that they have websites which enable them to buy online and that it's secure, it's easy, they can get discounts ... All of these issues persuade the customer because he will buy online from a company if it is known to him. (Business manager)_

Moreover, if all of these parties fulfill their roles as outlined above, but users remain anxious and ignorant of the issues and the technology of e-commerce, nothing will have been gained. Users should seek to educate themselves and to gain knowledge relevant to the use of e-commerce websites in order to overcome such worries. Part of the user's responsibility is protecting his private data. For example, one participant said:

_... but if the user trusts his friend and gives him his password, then it is his responsibility if any changes happen to his account (Security Manager)._

The next figure shows all categories that were found within the fieldwork (including the customer and the organization perspectives, and their associated concepts (except the tangible and intangible security features due to size of the list, they were tabulated in Table 6.1).
Figure 6.12: Factors that influence on e-commerce security effectiveness from the customer and the organization perspectives.
6.4 Relationships between categories and the core category

In grounded theory analysis, the interrelationships are addressed at category level. Cooperative responsibility is the core category which resulted from the data, and it is this factor which appears to link all other categories, combining customer and organisational perspectives. Figure 6.13 represents the interrelationships between the categories. Symbols (R1, R2,...R7) were assigned for each relationship. Depictions of these interrelationships are presented below.

Figure 6.13: Interrelationships between categories that influence on e-commerce security effectiveness from the customer and the organization perspectives
R1. Cooperative responsibility drives the effectiveness of security in e-commerce through cooperation between the entities involved. There is responsibility on the part of organization (i.e. management and technical staff), of users, and of the public and private sectors (e.g. government and banks).

R2. Social communication constitutes and causes positive and negative psychological aspect of security. For example, media disseminates a negative picture of the use of e-commerce through the propagation of bad news stories such as stolen money and fraud, causing customers to become fearful and instilling a reluctance to use e-commerce. An example of the positive effect of social communication is the dissemination of success stories about transacting on a certain website securely which leads to a reduction in the feeling of fear.

R3. Social communication constitutes and causes positive and negative perceptions of intangible security indicators. For example, past experiences with certain websites and success stories encourage other people to try e-commerce because of recommendations concerning the security and credibility of a certain website. Similarly, word of mouth between users about failure stories with certain website causes a bad reputation towards that website.

R4. Social communication constitutes and causes positive and negative perceptions of tangible security features. For example, word of mouth between users leads to perceive either positively or negatively that the padlock is a criterion for differentiating a secure website from an unsecured.

R5. Users’ characteristics constitute and cause positive and negative psychological reactions to security. For example, users who do not have enough knowledge could unwittingly give their credit card details to a fraudulent website; the resultant feeling of fear and powerlessness to control the transaction could make them reluctant to repeat the experiment. Similarly, users who have experience of transacting online and have the ability to evaluate whether or not a website is secure can reduce the possibility of risks happening leading to great use of websites.
R6. Users’ characteristics constitute and cause positive and negative perceptions of tangible security features. For example, knowledgeable and experienced users have the ability to check whether certain websites are secure by checking the security certificate. Similarly, unknowledgeable and inexperienced users are unable to check the tangible security features on the website such as security certificate and the presence of an “s” in https in the address bar.

R7. Management commitment supports implementation concerns. The expenditure on security involves support from higher management, together with the cost of security tools, of training security managers and of the integration of a secure EPS.

Figure 6.14 shows the resultant model of the categories, concepts and their interrelationships. It provides answers to the third research sub-question, where some categories are the result of the integration of the customer and organisational perspectives.
Figure 6.14: Research model of the effectiveness of e-commerce security from customer and organisation perspectives, resulting from grounded theory analysis
6.5 Conclusion

This chapter has presented the results of the data analysis by applying the grounded theory procedures, where categories and concepts are linked systematically by constant comparative analysis between the codes. The research model shown in Figure 6.14 summarises the findings. Excerpts from the participant’s responses were provided to confirm the emergence of the categories and that they are illustrative of the data. The next chapter will conclude the thesis by providing a critical discussion of the findings, an indication of the study’s contributions and an evaluation of the research.
Chapter 7: Conclusions

This chapter presents a critical discussion of the research findings and makes comparisons between the findings and those reported in the academic literature. It specifies the main contributions made by this research, proposes future research work and presents the limitation of the current research. It also evaluates the quality of the research process.

7.1 Critical discussion and implications

Based on the research findings presented in Chapter 6, the following implications for e-commerce and security can be drawn; these have been organised into fifteen issues.

Issue 1: The conflict between the actions of organisations and those considered important by users

The research findings showed that some of the participating organisations indicated their concerns about security by stating on the first page of the website that it was 100% secure (see Section 6.3.7). For example, one participant stated that their website then guides their customers to check whether a padlock symbol appears when a transaction is performed, advising them that if so, then the website is secure. This raises the question of whether such advice is sufficient to convince a customer purchasing online or performing online transactions. In essence, while it is important, it may indeed not be sufficient; a responsible company should, among other things, explain website security to its customers, not merely presenting a logo or using a short sentence to state that it is secure. They need to make clear what the padlock means, what technology is used to encrypt the data and what protocols are applied. This trend might be realised by the next generation of users. One participant from an organisation pointed out that customers' concerns are considered at the service level (see Section 6.3.1). If this is accepted as a premise, then it should be considered that the customers' only concerns are for the quality of the service provided on the website and whether it is easy to operate. In essence, this can be refuted by the argument that some users know the meaning of security indicators on websites, so that in this context new thoughts are required; a change of attitude is needed among technical staff, because they tend to underestimate customers' perceptions and their ability to understand what is involved. Thus, organisations exempt themselves from fulfilling their responsibility to educate their customers in
issues related to security.

On the other hand, the customers' responses revealed that they do not intensively check tangible security features, being more interested in knowing the identity of the other party; they want to know whether they are dealing with a national company which is well-known, famous and reputable, which are intangible features. If these questions are answered affirmatively, then the customer feels secure. For such customers, security is guaranteed on the basis of the abovementioned features (see Section 6.2.3). Consequently, more effort is required by the organisations in this matter, namely seeking strategies to make their websites better known and to boost their reputations. For example, if a customer wants to buy something from ‘Amazon’ does he then check whether the site is secure or not? This example would suggest that tangible security features on the website are not essential, but that the customer will decide to buy without checking, simply because he depends on the reputation of this website – and in this case the reputation of the company implies by default that the website provides the required security. This raises another question: does every company which has a good reputation actually guarantee the security of its website? In essence, it can do so only if the company is responsible for the protection of the customer’s data from its actions. For example, it was indicated by one participant that if a company’s website applies the best technology for the encryption of the customer’s data but then his private data is transferred by the website to another party without the customer’s consent, then the violation of security (i.e. confidentiality/privacy requirement) has come from the website itself (see Section 6.3.7), despite its supposed reputability; so the responsibility of the company for security should have two dimensions: protection of data from external hackers and from misuse by the parent organisation of the website itself.

**Issue 2: Tangible features do not totally guarantee security**

The organisational staff pointed out that there is no way to judge whether a website is secure or not (see Section 6.3.1). The justification for this doubt is that while security features (e.g. SSL or security certificates) of the website may mean that its operator has an honest stance towards its customers, that their data is encrypted for transmission, that the website’s identity is authenticated by a third party and that this, as reported by one participant, means that they do not deceive their customers and that the website undertakes to provide secure transactions, none of
this means that the company is able to guarantee totally that it will not be hacked or its security breached. In other words, as another participant stated, it is difficult for even well-known websites to guarantee total security. However, this leads to a reasonable enquiry: if there are no dependable criteria for distinguishing a secure website from an insecure one, what should the customer depend on to purchase online securely? In essence, this shows how such a significant role is played here by the intangible indicators of security such as the fame or reputation of the website, which is a high priority for many customers in deciding whether to buy online, since this assures him that the website’s operators undertake the responsibility to protect his data. This is what was asserted by the organisation’s view that customers’ concerns are about the reputation of the website, how well known it is, and how it scores on rating schemes, for example. It may be concluded that tangible and intangible security features are both important and both need to be considered by customers.

**Issue 3: Actions toward the psychological aspects of security**

There is a need to change the way that customers think and to reduce the effects on them of the psychological aspects of security. This can be achieved by raising consciousness among users of what they should understand about websites and of which security issues need to be checked and practised in order to reduce the feeling of fear; and by changing the misconceptions regarding the use of e-commerce. Some of the psychological aspects of security, such as the nature of e-commerce, which were discussed in Section 6.2.4, cannot be passed over; rather, the perception of the intangible factors of security, like the reputation of the website, can be affected by factors that exist physically. For example, the psychological feelings that affect the user as a result of the nature of e-commerce, related to anonymity and the absence of face-to-face interaction, can be reduced by the physical company in a number of ways. It can encourage its customers to buy online by offering discounts or vouchers and by telling them that the security of the website is insured, so that if a customer has a problem then he can make a claim, especially if he tries to buy something that he has already seen or touched in the company’s physical premises. This accords with the responses of some customers who said that if they want to buy online they prefer to deal with a nationally known Jordanian company which has a physical presence in the marketplace (see Section 6.2.3). So-called click-and-mortar websites, which conduct their business both online and offline, are deemed credible by such users.
Issue 4: Security perceptions affect practice

In essence, a customer's perception of security is not restricted by features to be checked on the website, but also comprises practices. Perceptions lead to practices that reflect these perceptions. One customer reported that there were some instructions which he had to follow in order to protect his private data, for instance changing his password frequently. He perceived a need to protect his private data and then he exercised that by following the instructions (i.e. practice) (see Section 6.2.2).

Issue 5: E-government is a prerequisite for successful e-commerce

It has been suggested earlier in this thesis that it is arguable that e-government is a phenomenon which increases the awareness of participation in e-commerce and not the reverse. In essence, this is a greater issue in countries new to e-commerce where e-commerce is still in its infancy and where every citizen who wishes to perform online certain traditional routine transactions such as paying bills or fees finds that there is no other way to do this than via the government's website. If payment is by a national electronic payment gateway that is secure and similar to that provided by the e-government website, then it is easy and feasible for customers to buy online, at least from any national business website which enables payment via a method similar to that provided by the e-government portal, because they have already experienced the latter. This would also enable businesses to use an EPS on their websites as an interface similar to that provided by the e-government portal, consequently enabling them to engage effectively in e-commerce, performing electronic transactions securely and at low cost (see Section 6.3.6). Therefore, the initial success of e-commerce in Jordan correlates with the initial success of e-government, both being accepted by customers and business with positive feelings concerning matters of security and trust on common EPS.

Issue 6: Conflict between national and international needs, and a tendency towards standardisation

The government has a vital role in providing a secure EPG. It was stated by one participant that websites launched in Jordan which are integrated with the international EPG would not even lead to "a national purchasing phenomenon" as the national one is being done for Jordanian users (see Section 6.3.6). Therefore, the government should consider this as being like any other project
applied at a national level by providing a secure EPG. Conversely, another participant said that their business (a website providing bookings and tickets) entailed dealing with an EPG and a third party which are international in order to be accepted by customers from all over the world, rather than only from Jordan (see Section 6.3.6), so the question arises as to how this can be reconciled with the remarks of the previous participant. It can be understood from the previous remark that the use of a certain secure EPS by a website depends on its business type and its target customers. However, while the notion of e-commerce should enable the customer to buy from anywhere in the world, in this case there is a need to start from a narrower national base within Jordan. The user who experiments with e-commerce transactions once can then repeat the experience from outside the country. But the previous contribution highlighted, besides the government’s responsibility, the issue of globalisation, whereby standards, rules and common protocols should be agreed and standardised throughout the world in regard to security, privacy and the regulation of e-commerce. These rules should be known to anyone from anywhere who wants to purchase online in a secure way. In Jordan, clear regulations and laws are also needed to control e-transactions between parties, and in activating these regulations, as one participant pointed out, “...we want to know if a problem happened between the customer and the merchant... does the arbitrator accept the electronic invoice and can they solve the problem?”

Issue 7: Images and designs reflect security and influence perceptions

One of the websites examined by a participant from one of the organisations features a logo depicting a lock and chain in an attractive and eye-catching image, which signifies security and which indicates that such a design can influence customers’ attitudes towards the website (see Section 6.3.7). The issue here is not one of ease of use of the website or one of the design being comfortable for the customer; rather, it is one of providing designs reflecting the meaning of security and which create the impression that the website is secure. Nevertheless, these designs do not in fact guarantee the security of customer’s data, as mentioned above (Issue 2). Indeed, tangible security features such as security certificates cannot totally guarantee security; consequently, these designs do not provide insurance, but serve only to make the consumer feel that the website is secure.
**Issue 8: Involvement of security managers in e-commerce development process**

The involvement of a security auditor or manager working with other personnel during the e-commerce development process is essential. However careful developers may be in respect of security issues, the security auditor has a viewpoint that may differ from the others, which will assist in building a secure and coherent e-commerce system; and as pointed out by one participant, a security auditor undertake the role of a hacker, addressing issues that may have been overlooked by the developers (see Section 6.3.6).

**Issue 9: Security insurance in e-commerce websites and the profits returned**

In order to provide a secure channel for online payments, a commercial enterprise has to find an IT provider to integrate the EPG with the website, which costs money and so reduces the company’s profits (see Section 6.3.6). One participant assessed this loss as being likely to exceed the profit generated, so that if the security insurance for a certain website involved more cost than the total profit that the company would make from providing the services on the website, then it would not be feasible to do business online. The participant stated that if a certain item is sold in a shop for 50 JD, the shopkeeper would expect a profit of 5-10% on the item, while if he wanted to sell the same item over the Internet then part of that profit would go to pay the EPG provider; and in some cases the whole profit might be needed. Thus, the expenditure on e-commerce security should be less than the profit returned by the company. This economic approach to security that has appeared here is also highlighted by another participant when he pointed out that “some websites in order to reduce expenditure do not get a security certificate from VeriSign, just to save $500.

**Issue 10: Cooperative responsibility drives the effectiveness of e-commerce security**

Cooperative responsibility, which emerges as a core category in this research, means that the success of e-commerce in respect of security, involves the responsibility of different entities which are complementary to each other; not a single responsibility. Thus, if the organisation applies the best technology to ensure the security of online transactions but the customers do not perceive that they are secure, then only part of that responsibility is fulfilled and this partial responsibility does not lead to the success of e-commerce. There exist responsibilities towards customers and by the customers themselves, as specified in Sections 6.2.5 and 6.3.7. Similarly, if
customers are educated about security issues and practices, and are aware of how to check whether a website is secure or not, but the organisation does not provide sufficient security for the website, then this is worthless and does not lead to effective e-commerce security. Another example, as mentioned above (Issue 1), is where the organisation fulfils its responsibility to apply the best security technology and the customers are aware of security practices on e-commerce websites, but the organisation uses customers’ private data in an illegitimate way. In such a case, security is violated by the organisation, in failing to fulfil its responsibility to protect customer data. The support of the government in providing a secure EPG for national businesses is a complementary responsibility and supportive of the effectiveness of e-commerce security. The mutual cooperation by banks and Jordan Visa as financial institutions with other entities like EPS developers, facilitating the use of credit/debit cards for online payment, is another form of responsibility. Banks have a significant role in promoting the culture of using credit cards, and this role so far is still inactive in Jordan. For example, one participant pointed out that the bank officer warned him from using his credit card for online shopping (see the quotation in Section 6.2.4). Therefore, there is a need to ensure the correct consciousness is in bank staff, in order to promote the culture of using credit cards and not frightening people in their use. Warnings from the banks, in the use of credit cards for online shopping, are aggravating the psychological state of security. In essence, the need for mutual responsibility is evident, where to establish e-commerce as a purchasing phenomenon at a national level involves the integration of the efforts of all parties.

Issue 11: Simulation by the virtual community of the real one influences customers’ perceptions of security

One of the main differences between e-commerce and traditional commerce is the community in which the process of buying and selling occurs. E-commerce takes place among a virtual community, but if it simulates the real community of traditional commerce to a high degree, then this contributes to the perception that the website is credible and consequently secure. For example, in regard to an auction website, one participant reported that there was a community café where sellers and buyers could chat, get to know each other, share opinions, provide suggestions, report transaction problems, recommend certain sellers and certain products, provide feedback, or request support from the website. All these activities are similar to those
which happen in traditional commerce, but now are conducted over the Internet. The community is virtual, but the buying and selling transactions are real and there are actual customers and sellers, which gives the site credibility and a sense of security. A new visitor will ask himself why other people would engage in such activities if it were not safe. One customer reported having heard that there are people who do business online and deal in shares online, adding that if it was not secure he did not think that they would do so. Therefore, the community, whether virtual or real, has an important role in constructing the perceptions of users and the more the virtual one simulates the real one, the more likely it is to be accepted.

**Issue 12: Security awareness, risk and time**

Time is an important factor in customers' awareness of security. This does not come suddenly but gradually, step by step, as indicated by those participants who suggested that it would take 3 to 5 years for e-commerce to become accepted as an ordinary purchasing phenomenon in Jordan, with customers feeling that it is secure. One customer indicated that such a perception comes with experience over time, not at once. The first difficulties that the new e-customer faces are how to deal with new technology, how to overcome the problem of the digital divide; then he can start dealing with promotional and service websites where he is required to provide data such as his name, address, telephone number and email address. At this point the customer begins to perceive some risks accompanying this activity, then when he starts to order products and pay by credit card or to engage in other online transactions, where the real risk becomes greater, his need to feel secure increases; so his perceptions change at each stage. Therefore, enhancing the customer's perception of security involves a sequence of time, given that the customer does not understand the risk completely at once, but step by step, and as the volume of risk and the need for security awareness are differs at each stage.

**Issues 13: issues related to the national EPS**

Although IT solution providers have recently developed a national EPS in Jordan, to increase its adoption it needs to overcome some obstructions such as reducing the cost of adopting this service for a business, the provision of facilities by banks to increase the culture of using a credit card, and making the procedures for online payment easy for customers to use and understand. There is a marketing role for the IT provider to promote the new national EPS with government
support. This is because there is a lack of promotion between business and other organisations, and this was apparent when one participant asked: “Do you know that until now there has been no Arabic electronic payment gateway?” Therefore, the national EPS provider should pay attention to local businesses in this development. In essence, there is a promotional responsibility on the part of the EPS provider in two directions: the first is setting strategies for encouraging businesses and other organisations that have not yet incorporated the EPS into their websites and the second is for businesses and organisations that already have EPS on their websites. In this case, the EPS provider should provide a competitive advantage over the international payment gateways, such as a lower cost than those from outside Jordan, showing that the best security solutions are applied and that the simplicity of procedures and support during integration are better. Also, showing that the national EPS being provided on the e-government website is similar to that which is being offered for businesses and organisations will help to foster customer acceptance, credibility and trust; as a result, the adoption of e-commerce will grow.

**Issue 14: Physical security as a requirement for e-commerce security**

Physical security means that physical goods (not digitized products) should be delivered to the customer with a guarantee of certain conditions. These conditions include the time of delivery and the conditional state of the purchased items. As reported by some customers, their concerns are around whether the items will be delivered or not, and whether the item is the right one or not (see Section 6.2.2). Physical security here has a different meaning from physical security stated by Kesh et al., (2005). For example, this will include accessibility to both the computers and servers, or safety from such equipment suffering damage, such as through a fire. The notion here, is that the concept of security is expanded to encompass the safety of goods delivered to the customer. Logical security includes, for example, security of transmitted data between customer and merchant, such as credit card details, which are encrypted and guaranteed by a third party such as VeriSign. However, the argument in this issue is neither logical security nor physical security (Kesh et al., 2005) is fully sufficient, rather physical security, as defined earlier, is another aspect that should be ensured. Similarly, as there are third party institutions guaranteeing logical security (VeriSign provides security certificates), there is a need for third parties to guarantee physical security through a secure delivery company. Thus, the customer is able to check whether the website is guaranteed by a third party before they order any items; for
example, a reference number can be used, or certificates provided, by the shipping company.

**Issue 15: Implications emerging from the research process per se**

There appears to have been very little research in the IS academic community in Jordan which has adopted a qualitative approach. In particular, the present study has used the grounded theory method, which is relatively new in this branch of science, so this research provides a rare example of this methodology for researchers in an area where most have previously followed a quantitative approach within the positivist paradigm. This restricted approach applies not only to academics, but to companies and customers, who are not aware of the importance of conducting interviews and discussions with them. This became apparent when the researcher was asked by some of the participants whether there was a questionnaire to answer and whether the questions could be sent and answered by email. It was clear that these respondents were not used to this type of research using interviews and face-to-face discussion, where the researcher did not set closed questions but instead established outlines and general issues in order to avoid limiting the interviewees to certain questions and so to permit new issues to emerge from the discussions.

### 7.2 Summary of Jordan Context

This research has explored the current attitudes to and perceptions of security on e-commerce websites from the perspectives of customers and organisations. The following points constitute a summary of findings in respect of the Jordanian context:

1. This research shows that the security challenge mentioned in prior studies pertains to the psychological feelings of customers.
2. The main problem that faces businesses in Jordan is providing a secure EPS.
3. The banks complicate the procedures of using credit cards in online payments in that the customer has to request this service from the bank; it is not provided by default.
4. The government, IT providers, businesses and banks have to take their share of responsibility for increasing the awareness of security instructions, features and usage in e-commerce, where this responsibility is still very weak.
5. Jordan has skilled IT personnel who export IT products and services, which means that the challenge is related to the use and acceptance of IT products and services by businesses and users within Jordan, not to the ability to develop these products and
services.

6. The number of people who use credit cards in Jordan is still very low: about 1.5 out of 6 million, supposing each person holds one card.

7. Business management needs to be mature in undertaking its responsibility to provide secure e-commerce by applying security standards, investing in the latest IT and security products, and providing advice for customers via their websites.

8. In Jordan, there is a need to pass clear laws and regulations governing e-transactions, then to put these into effect.

9. In Jordan, the success of e-government is a prerequisite to the success of e-commerce.

10. The interviewed customers/users are affected by social communications, in making the decision to buy online, recommending certain websites and establishing their credibility.

11. The interviewed customer/users tended to consider as secure and credible those websites run by companies which were well-known, national, reputable and not anonymous, and which also had a physical form (clicks and mortar).

12. Very few of the customers understood the tangible security features of e-commerce websites such as the padlock, security certificate or https, either what these meant or even that they gave an indication of website security.

13. For the customer participants, a sense of security was represented by protecting their sensitive information, in particular their credit card details, while they experienced anxiety concerning the receipt of the specific item requested and their ability to control and complete the process of e-transaction.

14. Security should not be seen as a product, but rather as the responsibility to provide a product, an undertaking to applying the standards of this product, investment in the product and educating the customers about the products offered via websites. For example, SSL is used to encrypt data transmitted between the customer and the merchant. This protocol (i.e. SSL (product)) enhances security, but this is not the crucial point; rather it is the awareness that a company should provide the standard version of this protocol on its websites by using at least 128 bit encryption, not 64 bit which is now easily broken, even though this requires the company to pay extra for this standard. It is a company’s responsibility to tell the customer about their efforts to protect his/her interests by applying the best security solutions, and that it is this which makes the
customer feels more confident.

15. People have incomplete experience of transacting online. This became clear when some of the participants stated their views and expectations about security in terms of ‘if... then... I would’: “If the website had... I would buy...”, or “I don’t have a credit card but I can differentiate between a secure website and a fake”, while a third said that if there were a third party acting as an intermediary to provide security then this would make him confident. These responses reported people’s expectations, not actual cases of transacting online.

7.3 Research Findings and Literature Review

This section addresses the relation between the research findings presented in Chapter 6 and the prior research. Generally, because little research has been done explicitly concerned with identifying the factors and their interrelationships influencing the effectiveness of e-commerce security from both the customer and organisational perspectives, as achieved in this thesis, there is little prior research to compare with the factors identified here and their interrelationships. However, the research results can be said to corroborate factors mentioned in the literature as influencing customers’ perceptions of security, such as the tangible features (e.g. padlock, security and trust logo and policies) while the present study also distinguished between tangible and intangible features. The research results also considered security to be essential at the beginning of the development process of an e-commerce system, supporting the work of Sengupta et al. (2005) and Zuccato (2007), where security is considered at the analysis and design stage. In addition, the support of top management that was mentioned by Kankanhalli et al. (2003), Yenisey et al. (2005) and Ho & Chang (2006) is also confirmed by the results of this research, which identified the role of top management in e-commerce security support.

The empirical data reveals two classes of e-commerce. The first, which can be called ‘full e-commerce’, entails the presence of an EPG and the risk that consequently arises. Security should be enhanced and ensured as a result, because it is a functional requirement in this situation. This involves high cost, in particular when a Jordanian business has to find an EPG provider from outside the country. On the other hand, the level of customer security awareness should increase. The second class, called ‘partial e-commerce’, does not involve any electronic transactions.
being used only for advertising and marketing. In this case there is no risk and no further cost, so no high level of security awareness and implementing technological security are required. However, this finding is at odds with that of the empirical research of Ruppel et al. (2003), which showed that security concerns are involved in all forms of e-commerce: transaction-based and promotional e-commerce websites.

Although the core idea of this thesis is investigating the security perceptions from the perspectives of both customers and organisations, the researcher has found it is difficult to put some of the participants’ responses with respect to trust away, where this terminology was used in their answers. The literature review provides theoretically and empirically a set of antecedent factors for trusting an e-commerce website. These factors include the characteristics of the online vendor, third-party certification, the individual’s propensity to trust, the influence of perceived risk, perceived security control (authentication, non-repudiation, confidentiality, privacy concerns and data integrity), perceived competence, legal framework, previous experience, perceived credibility, perceived ease of use, perceived privacy, perceived company reputation and willingness to customize products and services, perceived website usefulness, third party recognition, perceived investment, perceived similarity, perceived control, perceived familiarity and perceived size (Jarvenpaa et al., 2000; Cheung and Lee, 2000; McKnight and Chervany, 2001; Suh & Han, 2003; Corritorea et al., 2003; Koufaris & Hampton-Sosa, 2004; Walczuch & Lundgren, 2004; Teltzrow et al., 2007; Connolly & Bannister, 2007). Based on the above, it can be said that the perception of security from the customer’s perspective is a determinant of trust in the website, where perceived security is one among a number of factors increasing or diminishing the degree of trust. Customers’ perceptions of security in e-commerce are defined by Salisbury (2001, p.2) as “the extent to which one believes that the web is secure for transmitting sensitive information (e.g. credit card number)”; therefore the intangible features of security that were identified by customers and listed in Table 6.1 such as reputation, increase or diminish this belief: these features are also similar or indeed identical to some of the antecedent conditions for trust. In short, there is a recursive relation between security and trust this is one of the interesting issues which should be addressed by future research (see Section 7.5).
The psychological aspect of trust was identified in e-commerce literature, including beliefs, expectations, feelings and thinking. Stahl (2006) indicates, by referring to several authors, that the central aspect of trust is that it has to do with a psychological state of the trusting individual: it is an attitude that is normally based upon a belief linked to an expectation and often associated with certain feelings. Psychological aspects of trust are considered to be expectation and the context of online shopping (e.g. perceived security control, perceived privacy control, third party recognition and legal framework) are the two main factors that lead to an increase or decrease in the probability of performing an action based on trust (Lee et al., 2006). The psychological aspect of trust refers to the person who gives preference to ‘thinking’ or ‘feeling’, which determines whether he/she makes decisions by reference to facts or through the personal values of trusted peers (Hussain et al., 2006).

In this research, the psychological aspect of security was also identified, whereas no previous research had clearly considered the psychological aspects of the security of e-commerce. On the other hand, this psychological aspect of security includes concepts which emerged from the empirical data; fear, preconceptions, the nature of e-commerce and behaviour. However, there may be a similarity between the meaning of some concepts pertaining to the psychological aspects of security and those of trust; for example, preconceptions are similar to beliefs and expectations to some extent. However, since the present research followed grounded theory procedures, the psychological category including the concepts emerged and was named without any idea in regard to the terms of this category having existed before the fieldwork was conducted. Furthermore, some concepts emerging under this category, such as fear and behaviour, were not mentioned clearly in the literature (with respect the psychological concept on trust). Even though the emergent concept of “the nature of e-commerce”, explained in Chapter 6, was known, in this research this concept is interpreted in and related to the psychological state of the participants.

In respect of previous studies conducted in Jordan, this thesis has investigated in depth the nature of security that was mentioned by considering this issue as one of the main concerns for customers and businesses; it has specified the influencing factors and their impact on e-commerce security from both perspectives, thus providing insights into security concerns regarding e-commerce and directions to take in dealing with these concerns, based on the
meanings revealed by the participants themselves. Because this research is unique to Jordan, so the results cannot justifiably be compared with those of prior studies, none of which has covered the same research topic and objectives.

7.4 Research Contributions

This thesis has made theoretical and practical contributions and provides guidance for future research.

This thesis is the first of its nature in Jordan to focus on e-commerce security. It has also investigated empirically customers' and organisations' perspectives on e-commerce, whereas very little prior research has combined the two perspectives. Theoretically, this thesis identifies the factors and their interrelationships that influence the effectiveness of e-commerce security from the perspectives of customers and organisations. The following are the main factors and the interrelationships:

Factors
1. Implementation concerns
2. Cooperative responsibility
3. Management commitment
4. Users' characteristics
5. Social communication
6. Psychological aspect of security
7. Tangible and intangible features of security

Interrelationships
1. Cooperative responsibility drives the effectiveness of security in e-commerce through cooperation between the entities involved (i.e. user, management, government, and banks).
2. Social communication constitutes and causes positive and negative psychological aspects of security.
3. Social communication constitutes and causes positive and negative perceptions of
intangible security indicators.

4. Social communication constitutes and causes positive and negative perceptions of tangible security features.

5. Users’ characteristics constitute and cause positive and negative psychological reactions to security.

6. Users’ characteristics constitute and cause positive and negative perceptions of tangible security features.

7. Management commitment supports implementation concerns.

Theoretically, this thesis provides a critical framework of analysis for the existing e-commerce security literature from an IS viewpoint. This framework is constructed around four criteria: the nature of the previous contributions, the participants’ perspectives and the research method and type. These provide the justification for the current research and the basis for proposed future research work, where there is a gap in the existing literature. The research confirms some issues highlighted in Section 7.3 which have been validated by the literature. Furthermore, a wide range of implications are drawn from the collected data, which are presented into fifteen issues, and have been provided in section 7.2.

This thesis proposes an approach for integrating grounded theory methods with case study research which provides IS researchers with a guide to a suggested novel methodology which can be adopted in future research. The present research provides evidence of the successful application of this methodology.

In Jordan, the major factor that restricts the spread of e-commerce throughout the business world is the lack of secure EPG. One of the assertions made in this research is that most people interviewed considered the security concerns arising from online transactions to be the main reasons preventing them from accepting e-commerce. The other issue was the use of credit cards: some people still do not have these, or do not like to use them for online purchases, so there is a need to encourage a culture of using credit cards and for banks to provide facilities. In essence, the security tools used and actions taken by technical developers are not enough; there is a need for a raising of national consciousness regarding security in e-commerce in order to foster its
acceptance and engagement in it. The continuous development of technology alone, without the concurrent development of people’s consciousness would mean a divergence from, not a convergence towards, the point of the successful and effective implementation of security in e-commerce.

Practically, this research provides organisations in Jordan that intend to run their business via e-commerce with a way of thinking about this extensively by considering many issues, starting from the customer’s viewpoints; it shows them how to consider these and how to address the issues concerning the development of e-commerce websites. For example, whether integrating a website with national or international secure EPS; focusing on tangible and intangible security features security that serve as a stimulus for customers engagement on e-commerce; identifying new methods for mitigating the psychological state associated with customers, and the economic approach to e-commerce security. Therefore, establishing which factors should be considered in order to guarantee that security is provided, implemented, and perceived positively.

For practitioners and decision-makers in Jordan this research gives a clear conception and insight regarding the successful development of e-commerce by considering that security is the major barrier. Thus, it enables them to set effective and rational strategies and to recognise that the implementation of these strategies is not a single responsibility; rather, it is a national responsibility involving the public and private sectors, and these strategies concern the responsibility of all parties towards the customers. The strategies should also specify the procedures to be followed in order to increase the awareness of customers of security in e-commerce websites. The cooperation among different entities (i.e. users themselves, organisations, banks, government and media) helps in perceiving and implementing security in e-commerce.

The research has identified differences among Internet users concerning security, including the nature of psychological aspects of security in regard to the customers’ perceptions; and it is suggested that in order to promote the adoption of e-commerce there is a need to address and mitigate this psychological facet, which is the focal point for the customer. as shown by the empirical data. It has identified the role of the tangible and intangible factors in the awareness of
security, the influence of social communication in constructing the attitudes and beliefs concerning the credibility and security of e-commerce websites, and the customers' security needs and priorities. It draws the attention of the government and IT companies to the need to develop a secure EPS which is managed nationally in Jordan as an alternative to the international ones, thus enabling businesses to execute online payments while being accepted by local customers; it directs the EPS developers to promote the system among local businesses, directs the decision-makers in Jordan to speed the development of the e-government project, since it impinges on the success of e-commerce, and urges the promotion of the culture of using credit cards for online transactions.

Furthermore, the results of the research provide technical developers with some practices to be considered for developing secure e-commerce websites, an example being to develop a library of security breaches to be used by programmers to reduce the likelihood of future web breaches. Other suggestions are for the involvement of security managers during the e-commerce development process, utilising the tangible and intangible features that revealed by Internet users, presented in Table 6.1, developers and business managers should use these as a checklist in the assessment of e-commerce website security, providing a security solution centre on the website to solve customer's problems and answer their enquiries, establishing a rating system for e-commerce websites to increase customers' perceptions of security, and many others as set out in Section 6.2.6.

7.5 Future Research
The following are some suggestions for future research work to be undertaken in the light of the results of this study:

1. The model of factors and their interrelationships set out in Figure 6.14 could be tested and evaluated by other researchers, especially in developing countries, where they face the same challenges of security concerns that limit the use of e-commerce, particularly using quantitative research methods to produce statistical results, and identifying the significance of the factors and the relationships (e.g. factor analysis).
2. Further qualitative research could be conducted by applying the same procedures as were followed here to a comparative study of two developing countries, where new factors might be expected to emerge and contribute to extending the body of knowledge, or where the model which emerged could be compared with that proposed in the present study.

3. Another valuable area of future research would be to address the relation between security and trust, attempting to discover by empirical research whether the factors that influence security perceptions are the same that influence the level or nature of trust, whether only some are the same, or whether there is no relation, by investigating the same respondents' perceptions of the two issues together.

4. This research concerns itself within the Jordanian context; a statement by a participant from an organisation, believes that the trust between a customer and merchant is as nonexistent as it is between a customer and the Arabic Governments. This raises the question: is the approach for trustable e-commerce culturally dependent? Is there a global solution that will work in all cultural contexts? As globalization is in huge growth, at current time, this is an issue worthy of exploration.

5. One interesting element of research that should be conducted will be to examine the security features of Jordanian e-commerce websites, by evaluating the leading e-commerce websites in Jordan (telecommunication and mobile companies, banks, auction websites, and others). The evaluation of these websites is based on security features (tangible and intangible) that revealed by Jordanian Internet users, who would like to take these features into account when making a decision about transacting online (see Table 6.1). This is also based on a set of features that were reported in previous researches (see Table 2.1), identifying to what extent the examined websites meet these features. The evaluation of these websites provides both lessons and guidelines for companies who intend to run an online business or even setup an e-commerce website. It considers that do not, until now, consider security seriously, and that they should also take these issues into consideration, when looking at customer interaction and confidence. Additionally, this kind of research could identify new trends and implications from the examined websites.
7.6 Research Evaluation

In order to validate the research process and results, it is important to recognise that it is not a test whose outcome has a value of either 0 or 1, because of the nature of interpretive research, whose purpose is to explore human perceptions and views, which can be very varied. On the other hand, the interpretive research process is not an algorithm (Strauss and Corbin, 1990; Klein and Myers, 1999), so the validation should take this issue into account. The quality of this research can be evaluated according to the criteria that have been presented in Section 4.5:

1. **Credibility**: the subjects of the research were specified, as were the units of analysis; perceptions and viewpoints of customers and IT staff and managers were identified and investigated. The sampling was theoretical and purposeful rather than statistical, and based on relevancy to the research. The selection of participants was designed to deliver the research objectives. The researcher contacted the interviewees two months before the actual meetings and conducted electronic correspondence with the companies involved and the individual participants. Examples of corresponding emails were kept in order to increase the research credibility (see appendix D). The researcher spent time collecting data from the field, interviews were recorded on tape (wherever possible) and detailed notes were taken, and data was collected from multiple sources: interviews, documents provided by the participants, and websites (n=2) of the companies, whose security features were examined to see whether they were consistent with the evidence gathered during the interviews (triangulation). The researcher checked the informants’ responses for new emergent issues; for example, the security of EPS was discussed in the subsequent interviews with other informants to explore the issues arising from multiple evidences. The case study protocol was also defined. Furthermore, the researcher provided confirmation letter signed by two people, both native Arabic language speakers, to validate that Arabic and English texts have identical meaning (see appendix F).

2. **Transferability**: this thesis has set out in detail the procedure that was followed in the research, from defining the research questions, through the choice of the research paradigm, including the methods and techniques, to the findings and the results, giving
details of the context and setting (i.e. Jordan) in which data was collected, so that another researcher could apply the same procedures and might obtain the same results. Nevertheless, the generalizations made are to concepts and theories, not based on statistical generalization. The study has identified new concepts and relationships, highlighting implications so that although the results arise specifically from the Jordanian context, similar research could produce the same results or extend it to new concepts if it were conducted within the same context and followed the same procedures. As stated by Whalsham (1998), the generalisability in interpretive research involves developing theories and concepts and drawing out implications. Strauss and Corbin (1990) also state that the purpose of grounded theory is to build theory. Its generalisability is partly achieved through a process of abstraction: the more abstract the concepts, the wider is the theory's applicability (Strauss and Corbin, 1990). The categories in this research were conceptualised at a high level of abstraction, as shown in Chapter 6, and therefore might be transferred to another context.

3. **Dependability**: the research process has been set out clearly—in particular how the case study and grounded theory method were combined, justified and used for data collection and analysis—so, the methodology can be depended on and adopted by future researchers, as it was tested by the empirical research.

4. **Conformability**: samples of the participants' responses have been presented in this thesis to show how the concepts were extracted from the transcribed text and then how these were assembled to form the categories, which shows how each category is relevant and grounded in the data. Thus, a sequence of steps was followed which confirm that the results are based on the data and that the emergent concepts and categories were based on the meanings assigned by the informants themselves. The concepts are also seen to be interrelated in a systematic and reasonable way by the application of constant comparative analysis to the data. An example of a transcribed interview with a participant customer was provided in Arabic and English version including the extracted codes and concepts (see appendix A).
7.7 Limitations

1. The research reported in this thesis has followed the qualitative research approach, which depends on purposive sampling; the criterion for selection of the sample is that it should deliver the research objective; consequently it may be argued that the result of the research cannot be taken to represent the whole of Jordan. Indeed, decision-makers may prefer to see quantitative results and statistical analysis, which provide an overall picture. However, as stated previously, the aim of this research is not to quantify the problem, but rather, to obtain a better understanding of security concerns on e-commerce, from participants involved.

2. The study integrated case study research with grounded theory procedures for data analysis. The approach of Strauss and Corbin to grounded theory was adopted; however, the researcher did not follow their procedures precisely. Some may also argue that when using the grounded theory approach it is supposed that a theory should be developed. However, the purpose of using grounded theory procedures and techniques was only to categorise the data and identify the relationships, since this research was of the context-investigation type, and it is difficult to say that the model (Figure 6.14) in Chapter 6 is a theory applicable to different contexts (people, times, places) unless it can be repeated and tested.

7.9 Summary

Many prior studies have asserted that security is the main concern of both customers and businesses involved in e-commerce and a challenge to its success, particularly in Jordan. This study therefore investigated the current perceptions and viewpoints in respect of e-commerce security, seeking to identify the nature of security concerns from both of these perspectives, in order to gain a better understanding of the main concerns of the customer and so to provide the organisations with insights that would guide them to the implementation of effective strategies to deal with the challenges.

An interpretive-qualitative research was adopted in this research, which helps to make sense of and to understand the phenomenon in its natural setting. In analysis of the data, grounded theory
procedures were followed to categorise it and identify the relationships among categories in a systematic way. The adopted approach of using interpretive case study research integrated with grounded theory was justified as providing a fruitful complete research methodology. The results of the analysis satisfy the research objectives by identifying the factors that influence the perceived effectiveness of e-commerce security and the whole research process has delivered practical, theoretical and methodological contributions, as well as proposals for future research.
References


Onions, P., 2006. Grounded Theory Applications in Reviewing Knowledge Management Literature", *in*


Urquhart, C., 2001. An Encounter with Grounded Theory: Tackling the Practical and Philosophical Issues "; in


Websites:
- Basileiad Library, Manor College, UAS. [http://library.manor.edu/tutorial/empiricalresearch.htm](http://library.manor.edu/tutorial/empiricalresearch.htm) [Accessed 20-1-2008]
Get Safe Online: www.getsafeonline.org [Accessed 1-4-2007].
## Appendices

### Appendix A: Example of transcribed interview with a customer in English and Arabic version, and extracted codes and concepts.

<table>
<thead>
<tr>
<th>Codes and Concepts</th>
<th>Customer Interview (English Version)</th>
<th>Customer Interview (Arabic Version)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Researcher:</strong> have you bought anything or did you do any transaction online.</td>
<td>هل الشراء أثارت أي تعاملات إلكترونية؟</td>
<td>تذكرك الشراءات الإلكترونية؟</td>
</tr>
<tr>
<td><strong>Participant:</strong> yes I did, I bought tickets</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Researcher:</strong> In your opinion, is using Internet for buying products safe and secure? Why?</td>
<td>Do you consider online shopping safe and secure? Why?</td>
<td>هل تعتبر استخدام الإنترنت طريقة شراء معروفة ومطمئنة وماذا؟</td>
</tr>
</tbody>
</table>

### Trust

**People’s experience**

**Participant:** It depends, if the website that you would like to buy from gets the trust from the people... and if you hear that people use a certain websites and gain satisfaction, and the website is good, then I think I would do... I mean, not every website you can buy from... for example, there were many things available on the Internet I like, but because I do not trust these websites it makes me abstain from buying online. Any website that is commended by my friends, then I purchase from it. In general, it is an excellent way to perform shopping from your home, by clicking instead of going to the market and moving from one shop to another. Suppose you don’t like going to the market and visiting 5 or 6 stores, by using the Internet you can search the cheapest tickets and a suitable day for you to sit in your home and be comfortable

**Researcher:** What does security on e-commerce websites mean to you?

**Participant:** Well, security means once I’ve entered the security number, which is on the back of my credit card, no one can steal it, it is 3 numbers... mmm. It means that I get the goods I’ve ordered, not something else. You know, when I bought the ticket I received the ticket number. That’s all... while when you buy something else and you want it to be delivered to your home then you would like to be careful to receive what you

**Security meaning**

**Protection of private data**

**Receiving the same ordered products**

---

168
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information about security on the website</strong></td>
<td>You have to read about the website and see the evidence that there is security present, and that the website presents something to show you that there is security. Sometimes, the website provides you with information that makes you feel that this website is secure and also through transferring between the pages, step by step, until you get to the confirmation page. This gives me the feeling that they are serious and secure. Here, you feel the website lengthen the process and request details. But, as I told you, we hear from people that a website has been experienced and it is good, then this is better than going on an adventure (gamble and be victim). Although, I know a friend of mine who experienced purchasing over a website, but once he did not receive the order, so... sometimes something else happens. I hear that a padlock at the bottom of the page means 'this website is secure', but I can't tell you if this is actually secure or not. The main thing for me is what other people say, because they have more experience of these websites than me. Actually, I am reluctant to deal with a website for the first time because I don't want to be the victim.</td>
</tr>
<tr>
<td><strong>Feeling secure through Transferring between website pages</strong></td>
<td>A padlock at the bottom of the page means 'this website is secure', but I can't tell you if this is actually secure or not. The main thing for me is what other people say, because they have more experience of these websites than me. Actually, I am reluctant to deal with a website for the first time because I don't want to be the victim.</td>
</tr>
<tr>
<td><strong>Commendation from people</strong></td>
<td>A padlock at the bottom of the page means 'this website is secure', but I can't tell you if this is actually secure or not. The main thing for me is what other people say, because they have more experience of these websites than me. Actually, I am reluctant to deal with a website for the first time because I don't want to be the victim.</td>
</tr>
<tr>
<td><strong>Other's experience and Knowledge of security</strong></td>
<td>A padlock at the bottom of the page means 'this website is secure', but I can't tell you if this is actually secure or not. The main thing for me is what other people say, because they have more experience of these websites than me. Actually, I am reluctant to deal with a website for the first time because I don't want to be the victim.</td>
</tr>
<tr>
<td><strong>Fear to be victim</strong></td>
<td>A padlock at the bottom of the page means 'this website is secure', but I can't tell you if this is actually secure or not. The main thing for me is what other people say, because they have more experience of these websites than me. Actually, I am reluctant to deal with a website for the first time because I don't want to be the victim.</td>
</tr>
<tr>
<td><strong>Padlock</strong></td>
<td>A padlock at the bottom of the page means 'this website is secure', but I can't tell you if this is actually secure or not. The main thing for me is what other people say, because they have more experience of these websites than me. Actually, I am reluctant to deal with a website for the first time because I don't want to be the victim.</td>
</tr>
<tr>
<td><strong>No website is 100% secure</strong></td>
<td>A padlock at the bottom of the page means 'this website is secure', but I can't tell you if this is actually secure or not. The main thing for me is what other people say, because they have more experience of these websites than me. Actually, I am reluctant to deal with a website for the first time because I don't want to be the victim.</td>
</tr>
<tr>
<td><strong>Information provided from the website</strong></td>
<td>A padlock at the bottom of the page means 'this website is secure', but I can't tell you if this is actually secure or not. The main thing for me is what other people say, because they have more experience of these websites than me. Actually, I am reluctant to deal with a website for the first time because I don't want to be the victim.</td>
</tr>
<tr>
<td><strong>Reputation</strong></td>
<td>A padlock at the bottom of the page means 'this website is secure', but I can't tell you if this is actually secure or not. The main thing for me is what other people say, because they have more experience of these websites than me. Actually, I am reluctant to deal with a website for the first time because I don't want to be the victim.</td>
</tr>
<tr>
<td><strong>References to Security Company (Third party)</strong></td>
<td>A padlock at the bottom of the page means 'this website is secure', but I can't tell you if this is actually secure or not. The main thing for me is what other people say, because they have more experience of these websites than me. Actually, I am reluctant to deal with a website for the first time because I don't want to be the victim.</td>
</tr>
<tr>
<td><strong>Unknown identity (virtual)</strong></td>
<td>A padlock at the bottom of the page means 'this website is secure', but I can't tell you if this is actually secure or not. The main thing for me is what other people say, because they have more experience of these websites than me. Actually, I am reluctant to deal with a website for the first time because I don't want to be the victim.</td>
</tr>
</tbody>
</table>
number or brand name of this company in the security company’s list... Not merely a stamp, but a reference number... This method makes buying over the Internet secure.

You know what, it could be a hacker build a website and put these stamps on and symbols, but in reality they are fake. But when a reference number is used, which refers to the security company, then this builds more trust because many fake and deceitful transactions are happening over the Internet, because you deal with unknown people.... you deal with something virtual.

Researcher: Do you feel confident in the security of e-commerce transactions? Why?

Participant: If I deal with a new website which is not known to me I don’t feel confident because I have got a large amount of money in my account. Why should I take risks by myself and lose my money? Here you could lose more than you gain.

Researcher: Do you think these websites (you trust them) use your personal information in a right way

Participant: Well, I don’t guarantee, I mean it is likely that a website I buy from sends my data to another company and tells them that this is a valuable customer and that they may buy from your website. Perhaps this website has a relation with other websites, or sometimes one owner of many websites send you information you did not request, because they know you from the first company; I mean, a website for mobiles and one for cars and other for booking tickets, so if one website sees that you are trusted then they may pass on your data. It opens up business for other companies and websites.

Of course, if I want to buy something and it attracts me, then I have to provide them my name and address, and where the order should be delivered, but if I don’t want to
**Company responsibility**

<table>
<thead>
<tr>
<th>buy, then I don’t give them my information; why would they need it? But, in order for there to be trust between the customer and the company, they should ask the customer whether they would like to send your details to other commercial websites or not. Some websites ask you about this, once happened with me.</th>
</tr>
</thead>
</table>

**Researcher:** What have you chosen (i.e. Would you like to receive promotional emails?)

<table>
<thead>
<tr>
<th>Participant: Of course not, nothing necessary for that, then, I receive a hundred of emails</th>
</tr>
</thead>
</table>

**Researcher:** Do you want to add something? I would like to tell you that trust comes from the dealing, and not by talk; I mean, how much you read that strongest website... all it is speech unless you experiment with the website and you hear from other people’s experience, and sometimes you need to hear from more than one person, as sometimes one person may have been successful and another one failed.

If I want to enter my personal information then I have to deal with a secure website because you are dealing with something intangible in your hands, and it is virtual.

I think companies should increase their security on the Internet and make you feel that there are promotions to inform people that their website is secure... our website can’t be hacked but it is still something difficult. Perhaps when you have had your identity stolen, or something wrong happened to you, then the company can compensate you, but perhaps users are not honest, so the company should monitor all transaction and accounts.

In fact, making payments over the Internet facilitates many things, especially for those who do not have time to pay water and electricity bills, so why should I leave my job; however, through e-commerce we will face another problem, where many companies will make employees redundant, resulting in another problem: unemployment.

<table>
<thead>
<tr>
<th>في بعض المواسم نعم بتسال ومرة صارت معي طبعا لا لأنه ما في داعي يعني بعدا يصننني من ذات الاميلات هل تريد ان تضيف شيء؟ borne افكك ان العقلة نانا بالتعامل ولي بالحكى يعني الى ما حد ما تقترن ان اقة موقع وامن موقع نطل كلام بكالم حتى انا تحرر الموقع وتمع من خبرات الناس واحيانا تحتاج لأن تسعى من أكثر من شخص لأنه ممكن شخص جرب ونجحت معه ولشخص آخر فشلت معه لذلك انا لما بادي ادخأ معلومي لا بد أن يكون في امان يعني انت بنتعامل مع شيء ملموس بينينا مع وهم اعتقد ان الشركات لا بد ان تزيد الأمن على الشبكة وتشعر انه في اعتلالات في عاذا انه موقعنا امن موقعنا لا يمكن افتتاحه لكن يبقى الأمن صعب لربما ان تسرق او شيء بلخطأ يحدث معك ممكن تكون صالحة وممكن الشركة تعوضك لكن لا بد ان يكون عندنا اجهزة رصد ومراقبة على الحساب والمعاملات</th>
</tr>
</thead>
</table>
Appendix B: Ethical Form
De Montfort University

Faculty of Computing Sciences and Engineering

Advance approval of activities involving human research ethics

Title of Activity
Investigating the Factors that influence the effectiveness of E-Commerce Security in Jordan

Researcher / Student Name: Mohanad Ali Halaweh

Supervisor Name: Dr. Christine Fidler

Brief description of activity objectives
This study is about E-commerce security in Jordan. Within this research, a qualitative, case study approach will be adopted to identify an initial possible framework that interrelates technical and non-technical factors that are found to significantly influence an appropriately selected Jordanian business. The case study method will involve interviews with people.

If the review of the activity results in major ethical issues being identified (outcomes 3 or 4) describe the issue(s) and procedures in place to address them (outcome 3 only)

The activity results in minor ethical issues only.
Advance approval of activities involving human research ethics

Review of activity

Has the research proposal identified any of the following research procedures?

2. Using archived data in which individuals are identifiable
3. Researching into illegal activities, activities at the margins of the law or activities that have a risk of injury

If any of the above occur does the proposal satisfactorily identify the ways in which the researcher/student will be dealing with the following (tick boxes for "YES"):

- Providing participants with full details of the objectives of the research
- Voluntary participation with informed consent
- Written description of involvement
- Freedom to withdraw
- Keeping appropriate records
- Signed acknowledgement and understanding by participants
- Consideration of relevant codes of conduct

Do the procedures identified necessitate formal third party assessment? NO
If so has the assessment been carried out? N/A

There are four possible outcomes from reviewing the activity against the three categories and the procedures in place:

1. no ethical issues
2. minor ethical issues which have been addressed and concerns resolved
3. major ethical issues which have been addressed and concerns resolved
4. ethical issues that have not been resolved

Tick the outcome of the review: 1 □ 2 □ 3 □ 4 □

Authorisation

- The reviewer authorises those activities in the first three outcomes.
- Activities in the third outcome are reported for information only to the Faculty Committee
- Activities in the fourth outcome are submitted to the Faculty Committee for resolution

signature of researcher/student
signature of supervisor
authorising signature
Appendix C: Formal Letters
To whom it may concern:

Dear Sir /Madam,

I am writing in support of Mohanad Ali Halaweh, a Jordanian National, who is currently studying for a PhD in Information Systems with myself, as his first supervisor, at De Montfort University, Leicester, in the UK. Specifically, Mohanad is investigating e-commerce security issues within Jordan (as a case study). The findings from this research will be of immense benefit to Jordan and other countries in their continued pursuit of effective e-commerce.

To perform this research, it is vital that Mohanad gains a sound understanding of the views and opinions of key personnel within business regarding e-commerce implementation, and it is therefore for this reason that we require your input and support. I would be extremely grateful if you would allow Mohanad to gather the information he requires from you regarding e-commerce implementation and security within your organization. Please be assured that any information gained from you will be used solely for the specific purposes of this research, and will be treated with the utmost respect, and in accordance with appropriate ethical practices and legislation.

I hope that you will be able to help Mohanad in his research, and I thank you in advance for your cooperation in this matter.

Yours faithfully,

Dr. Christine Fidler BSc (Hons), MBCS, CITP
Principal Lecturer & Research Supervisor
School of Computing
Faculty of Computing & Engineering Sciences
De Montfort University
To whom it may concern:

Dear Sir /Madam,

I confirm that Mohanad Ali Halaweh, Jordanian National, is currently studying for a PhD in Information Systems with myself, as his first supervisor, at De Montfort University, Leicester, in the UK. Specifically, Mohanad is investigating e-commerce security issues within Jordan (as a case study). The findings from this research will be of immense benefit to Jordan and other countries in their continued pursuit of effective e-commerce.

I am requesting that you would support Mohanad in his research work, and therefore that you would allow him to gain the information he requires from you regarding e-commerce and its implementation within your organization.

Please be assured that any information gained from you will be used solely for the specific purposes of this research, and will be treated with the utmost respect, and in accordance with appropriate ethical practices and legislation.

I hope that you will be able to help Mohanad in his research, and I thank you in advance for your cooperation in this matter.

Yours Faithfully,

Dr. Christine Fidler BSc (Hons), MBCS, CITP
Principal Lecturer & Research Supervisor
School of Computing
Faculty of Computing & Engineering Sciences
De Montfort University
Appendix D: Samples of email correspondence with the participating companies
RE: Regarding interviews arrangement

From: linahussein@eskadenia.com (linahussein@eskadenia.com)
Sent: Monday, January 01, 0001 2:00:00 AM
To: LinaHussein@eskadenia.com

Dear Mrs Lina,

Thank you a lot for your help, and this actually will be acknowledged.

The date that you have specified is very proper to me but could you tell me the exact time. I suggest initially 1 to 1 and 1/2 hour is enough for each meeting.

Regards,
Mohanad Halaweh.

---

From: 'Lina Hussein' <L/naHussein@eskadenia. com>
To: "Mohanad Halaweh" <ha//awahl @hotmai/. com>
CC: "Mohammad Al-Rousan" <M. A/Rousan@eskaden/a. com>, AbuNada " <abunada@eskadenia. com>
Subject: RE., Regarding interviews arrangement
Date: Thu, 14 Jun 2007 17:27:20 +0300

Dear Mr Mohanad,

It would be a pleasure to assist you in your PhD thesis in any way possible.

In this regard, two colleagues of mine in the Internet Software Department will be meeting with you regarding the surveys you have.

Please advise on the amount of time required.

I initially propose to start meetings sometime on Tuesday 19th or Wednesday 20th June 2007.

Best Regards

---

ESKADENIA® Software
Lina Hussein
Manager - Communication
Tel: +962 6 5510717 - Ext: 124
Fax: +962 6 5510719
www.eskadenia.com
IT Solutions to the Global Market

ESKADENIA® Software is active in the design, development and deployment of a range of software products in the Telecommunications, Enterprise and Internet Applications areas. The company is based in Jordan and has sales activities in Europe, the Middle East and Africa. ESKADENIA is a product and market-oriented organisation that assists enterprises and promotes businesses by use of highly effective IT strategies, tools and solutions, and more than 80% of its sales are exported to the Global IT market. ESKADENIA strongly believes that a company's achievement is derived from the success of its Human Resources and the commitment to quality and excellence that each one holds strong to. ESKADENIA endeavours as a team to maintain quality, strive for customer respect, build up perseverance, and foster innovation while handling any task or challenge.

---

Legal: This communication is intended for the above named person and is confidential and/or legally privileged. If it has come to you in error, do not take any action based on it, nor copy or show it to anyone: please delete it and inform the sender immediately. ESKADENIA Software is not responsible for any political, religious, racial or partisan opinion in any correspondence conducted by its domain users, therefore, any such opinion expressed, whether explicitly or implicitly, in any sent correspondence or context, is not to be interpreted as that of ESKADENIA Software.
From: Mohanad Halaweh [mailto:hallawah1@hotmail.com]
Sent: Tuesday, June 12, 2007 4:38 PM
To: Lina Hussein
Subject: Regarding interviews arrangement

Dear Mrs Lina,

Thank you a lot for your cooperation.

The main aim of my research is to investigate the factors that influence on E-commerce security effectiveness, and this will focus on the implementing of secure E-commerce websites from expert IT people, business employees viewpoints, and the perception of security from customer’s viewpoint. To obtain in-depth and relevant information about the question of the research, a series of semi-structured interviews will be conducted, which also allow the informants the opportunity of supplying their opinions, knowledge and experiences on a wide range issues.

The key issues of the research are:

1. Implementing Secure E-commerce websites.
2. Perception of security on E-commerce websites (customer’s viewpoint).

The importance of that is to lead the organizations to use certain security solutions that support customer’s objectives and perception in order to reduce the gap between what is being implemented within technology by organizations and what is perceived by customers.

Mrs Lina I think the key people that could answer my questions those who are responsible for developing and implementing E-commerce websites and those who have knowledge about security requirements in EC, and business analysts.

I hope that is sufficient for your request. Formal letter from the university will be brought in order to show that the collection of data is only used for scientific research purpose.

Regards,

Mohanad Halaweh
Research student, PhD
Information system Dept
School of Computing
De Montfort University
Leicester, UK
hallawah1@hotmail.com or
Mohanad.halaweh@learner.dmu.ac.uk
Mobile No. +44-7722197639
RE: Dear Mr. Dabbas

From: Hussein Dabbas (hussein.dabbas@rj.com)
To: 'ahmad abu Ragheb' (ahmad.aburagheb@rj.com); mai.omeish@rj.com
Cc: 'Mohanad Halaweh' (hallawah1@hotmail.com)

Dear Ahmad and Mai

I believe you can be of more help to this PHD candidate, can you please contact him
regards

Hussein Dabbas
V.P. Marketing, Sales & Services
Royal Jordanian Airline
P.O.Box: 302
Amman, Jordan
Tel: 962-6-520-2500
Fax: 962-6-569-8816

From: Mohanad Halaweh [mailto: hallawah1@hotmail.com]
Sent: Sunday, May 06, 2007 2:53 PM
To: hussein.dabbas@rj.com
Subject: Dear Mr. Dabbas

Dear Mr. Dabbas,

I am Jordanian research student/ PhD Computer and Information System/ UK. I am doing research about Security in E-commerce (Jordan as a case study). I discovered Royal Jordanian as one of the first companies in Jordan supports E-commerce application. I would like to ask you if I can conduct an interview with you and other employees within Royal Jordanian (team who is responsible for implementing and developing the website of RJ) in respect to security issues in E-commerce form different perspective: technical, organizational and customer viewpoint.

Formal letters from the university will be provided in order to show that the aim of this research is for scientific purpose.

Any details about the objectives of the research will be showed.

I am looking forward to receiving your consent.

Sincerely,

Mohanad Halaweh
Research Student, PhD
School of computing,
Dear Mr. Sadek, Subhi,

Thank you so much.

Regards,
Mohanad.
Dear Mr. Sadek,

I would thank you for your cooperation. Please, can you send me an overview about the security requirements and objectives on PayOne (Electronic payment Gateway system) and how they are fulfilled and what security techniques, tools and measures that were applied on this project.

Best Regards,

Mohanad Halaweh
Research Student, PhD
Information System Dept.
De Montfort University
Mohanad@dmu.ac.uk
hallawah1@hotmail.com
Jordan: +962-795009308
Uk: +44-7722197639
SECURITY PERCEPTION IN E-COMMERCE WEBSITES –
A CUSTOMER’S PERSPECTIVE

Mohanad Halaweh, Christine Fidler, Steve McRobb*
School of Computing
De Montfort University
Leicester, UK

ABSTRACT
The aim of this paper is to explore the customer’s perception of security in e-commerce websites in Jordan, since security is generally the main concern which restricts customers engaging with e-commerce. This paper resulted as part of a PhD project. One category of the initial results emerged from the first data collection, showed that security concerns for customers are a psychological matter, which will be highlighted in this paper. A qualitative research approach was adopted, since the research seeks a viewpoint and understanding of user perception, with the grounded theory method being used to analyse the data.

KEYWORDS
E-commerce, security perception, psychological aspect of security, grounded theory

1. INTRODUCTION
According to the Gartner survey of 5,000 online U.S. adults in 2006, about $913 million in e-commerce sales were lost that year because of security concerns amongst online shoppers (www.gartner.com). Customers do not perceive e-commerce sites as having sufficient security and they do not have enough knowledge about security features that need to be in place on e-commerce websites. This was confirmed by the Get Safe Online survey that was conducted through the UK in 2006, to investigate online behaviour and attitudes towards internet security. It showed that only 27% of respondents said ‘I am very knowledgeable about PC security and confident about staying safe online’ (www.getsafeonline.org). Specifically for Arab countries, and according to Aladwani (2003), internet security was ranked the primary concern for customers and business managers with respect to the usage of e-commerce. Al-Sukkar and Hasan (2005) conducted research about internet banking adoption in Jordan; he mentioned one of the main concerns by customers and banks is security. Another study was carried out by Alsmadi (2002) to investigate the attitude of the Jordanian customers towards using the internet for online shopping. The results, based on 500 respondents, suggested that online transaction security was a key factor in the willingness of people to shop online. In Jordan, until this study was conducted, no previous studies have investigated the perception of e-commerce website security from a customer’s perspective. Thus, this research is the first of its nature in Jordan to shed light on this issue. Salisbury (2001) defined a customers’ perception of security on e-commerce as “...the extent to which one believes that the Web is secure for transmitting sensitive information” (p. 2). This paper focuses on the psychological aspect of this perceived security that was identified from the fieldwork.

2. RESEARCH METHOD
A qualitative approach was employed in this research and the grounded theory method of analysis, as defined by Strauss and Corbin (1990), was adopted. Qualitative research is subjective in nature and involves examining and reflecting on meanings and perceptions in order to gain an understanding of social and human activities. Qualitative research assists the researcher in understanding phenomena in depth.
narrowing to certain predetermined hypothesis that need testing to see if they are true or false, as in quantitative methods. As the aim of this research was not to quantify the phenomena but to develop a better understanding of the customer's perceptions, a qualitative approach is appropriate. A total of 10 interviews were carried out with customers. The questions that were used with customers include 'have you bought or performed any online transactions, and if not, why not?', 'what does security mean for you?', and 'how can you check a certain website is secure or not?' The nature of these questions is open; therefore, the researcher was not limited to set answers and the research took on an exploratory nature. All of the recorded interviews were transcribed and converted to text, and then the text was ready to be analysed using grounded theory.

3. PSYCHOLOGICAL ASPECT OF SECURITY

From the application of grounded theory analysis (i.e. by constant comparative analysis of data segments and the continuous asking of the question ‘what does this piece of data mean?’, and reflecting on the answers received, and then assigning and labelling the emergent concepts, as illustrated in Table 1, for those meaningful data segments), data showed that there is a psychological aspect to security, as far as the customer is concerned: the psychological aspect incorporates the feeling of fear, the need to feel that one's money is secure, and the ability to control the process of payment and performance of online transactions. There is a widespread perception among the interviewed participants that current e-commerce does not meet these concerns.

Customers have a preconception that buying and selling over the internet is risky. This is partly due to the (1) customer's perception that use of e-commerce for buying and selling is vulnerable and that there is a high probability that money will be lost, and (2) due to the intrinsic nature of e-commerce, being remote rather than face to face, and therefore the user does not touch or see anything but the computer screen; what lies behind this screen is unknown, and this makes people very skeptical. The psychological aspect of security also incorporates the customers' behaviour towards using e-commerce. For example, one customer indicated that they were cautious and kept their passwords from being disclosed, while another saw the following of instructions as protecting him. Table 1 provides several further examples of customer answers. It shows quotations matched with extracted and named concepts, which in total defined the psychological aspect of the security category.

Table 1. Example of customer's responses and the extracted concepts for the Psychological Aspects of Security category

<table>
<thead>
<tr>
<th>No.</th>
<th>Customer’s responses</th>
<th>Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Actually I am reluctant to deal with a website for the first time this because I don’t like to be the victim</td>
<td>Preconception, fear</td>
</tr>
<tr>
<td>2</td>
<td>but if that happened I will fear more and I abstained from buying online</td>
<td>Fear</td>
</tr>
<tr>
<td>3</td>
<td>Because you are dealing with the unreal world, you don’t know the identity of the other side, and you just have a screen</td>
<td>Nature of E-commerce</td>
</tr>
<tr>
<td>4</td>
<td>Some websites says 100% secure, in my opinion not all of what is written is believed, it is rubbish speech</td>
<td>Preconception</td>
</tr>
<tr>
<td>5</td>
<td>...... but I tried the first time and then I repeated because I had had experience, but the first time the fear barrier was with me</td>
<td>Fear</td>
</tr>
<tr>
<td>6</td>
<td>Why shall I take risks and lose my money</td>
<td>Preconception</td>
</tr>
<tr>
<td>7</td>
<td>I found black background webpage come out suddenly. This meant something to me - horrible and something relevant to a hacker, and this site is impossible to buy from</td>
<td>Fear</td>
</tr>
<tr>
<td>8</td>
<td>I fear dealing with unknown website because there is unreal website and then they are making fraud</td>
<td>Fear, nature of E-commerce</td>
</tr>
<tr>
<td>9</td>
<td>I hear that hackers, who are very clever, steal money and your identity</td>
<td>Fear, preconception</td>
</tr>
<tr>
<td>10</td>
<td>If they request unreasonable and unexpected information I don’t deal with them because this makes me doubtful</td>
<td>Behaviour</td>
</tr>
<tr>
<td>11</td>
<td>But in general people should be very careful</td>
<td>Behaviour</td>
</tr>
<tr>
<td>12</td>
<td>On the other hand ,I have two accounts one with a small amount in, just in case an error happens</td>
<td>Behaviour</td>
</tr>
<tr>
<td>13</td>
<td>Well, the reason I have no experience in how I can deal with a page will come out when I select item for purchasing</td>
<td>Fear (out of control)</td>
</tr>
</tbody>
</table>
There are some instructions I should know as a customer to protect myself from any person. On the other hand, this requires some caution from me to keep my passwords from others. Well, some of them secure and some of them fake, so internet users should be cautious; for example, many websites send me promotions saying get your gift such as mobile or computer, it requests your details...... but I don’t give them because how I can win something without paying, so these websites lie and just want to get your information.

In some cases the expressions of the participants through face to face interaction gave the researcher a real and direct interpretation of body language and feelings, which text does not always sufficiently reflect, with respect to psychological concerns; the third quotation provides an example of this situation, where the respondent’s body language presented a far more powerful message than that conveyed in the written narrative.

A psychological aspect of trust has already been identified in e-commerce literature including beliefs, expectation, feeling, and thinking. Stahl (2006) indicated, by referring to several authors, that the central aspect of trust in e-commerce is that it has to do with a psychological state of the trusting individual (i.e. the buyer), and with that being trusted (i.e. the e-commerce site). He continues by stating that trust is an attitude that is normally based upon a belief linked to an expectation and often associated with certain feelings. Psychological aspects of the trust consider expectation and the context of online shopping (i.e. perceived security control, perceived privacy control, third party recognition, and legal framework) as the two main parameters that cause an increase or decrease in the probability of performing an action based on trust (Cheung and Lee, 2003, 2006).

In this research, a psychological aspect to e-commerce security was identified. No previous research had uncovered psychological aspects to security perception with regard to e-commerce. The psychological aspects identified in this research, based on the customers’ responses to interview questions as presented in Table 1, include elements which are not included in the existing trust literature, and comprise preconceptions, nature of e-commerce, fear, and behaviour of consumers. However, there is similarity between the meaning of some concepts which pertain to the psychological aspects of security and some of those mentioned with respect to the psychological aspects of trust; for example, preconceptions are, to some extent, similar to beliefs and expectations. However, since the researcher followed the grounded theory procedures verbatim, it was only after the psychological category, and the underlying labelled concepts, emerged from the fieldwork that it became apparent that consideration of the literature on the psychological aspect of trust was necessary. In addition, there are concepts under this emerged category regarding customer fear and behaviour, which was not mentioned clearly in the psychological aspects of trust literature. Even though the “the nature of e-commerce” concept is a known fact, in this paper this concept is interpreted to be linked to the psychological state of the customer.

4. CONCLUSION

This paper has focused on the customers’ perception of security towards e-commerce websites in Jordan. It revealed the psychological aspects of security concerns for customers, including emerged concepts such as fear, preconception, behaviour and the nature of e-commerce. This paper provides insight into the customer and their viewpoints of security, and therefore will aid practitioners to carefully consider these viewpoints, enabling them to set effective and rational strategies to mitigate the misconception of their perception. The effective addressing of the emerged psychological concepts can also form a worthy subject of further research, for example investigating ways that the fear can be reduced, and how the misconception in customers’ minds can be alleviated (for example, making shopping online simulate more closely the traditional off-line shopping experience).

One may argue that the number of the participants (10) in this study was low which can be seen as a limitation. However, the aim of this research was to achieve in-depth understanding rather than to focus on large sampling, and therefore the number was considered reasonable. The outcomes presented in this paper form only a portion of the results of the PhD research undertaken: further categories have been identified, but...
the researcher has provided only the quotations and codes that are relevant to the emergent psychological aspect of security category only.

REFERENCES


(www.gartner.com) [Accessed 10 June 2007]

(www.getsafeonline.org) [Accessed 10 June 2007]
Integrating the Grounded Theory Method and Case Study Research Methodology Within IS Research: A Possible ‘Road Map’

Mohanad Halaweh* Christine Fidler†
Steve McRobb‡

*De Monfort University, mohanad@dmu.ac.uk
†De Monfort University, cf@dmu.ac.uk
‡De Monfort University, smcrobb@dmu.ac.uk
This paper is posted at AIS Electronic Library (AISel).
http://aisel.aisnet.org/icis2008/165
INTEGRATING THE GROUNDED THEORY METHOD AND CASE STUDY RESEARCH METHODOLOGY WITHIN IS RESEARCH: A POSSIBLE “ROAD MAP”

Intégrer la théorie enracinée et la méthode des études de Cas dans la recherche en SI : une « Feuille de Route »

Mohanad Halaweh
School of Computing
De Montfort University
Leicester, UK
Mohanad@dmu.ac.uk

Christine Fidler
School of Computing
De Montfort University
Leicester, UK
cf@dmu.ac.uk

Steve McRobb
De Montfort University
School of Computing
Leicester, UK
smcrobboj@dmu.ac.uk

Abstract

Grounded theory is used by many IS researchers. Sometimes they apply it as a method and sometimes they apply it as a methodology. This different application stems from the debate between Glaser and Strauss, the originators of this theory. Some IS research implies the simultaneous use of case study and grounded theory. However, no conceptual/theoretical research for IS researchers yet specifies how grounded theory can be used as a method to be embraced within an interpretive case study strategy, to define a research methodology. This paper is therefore written to help IS researchers who are considering the use of grounded theory as a data analysis method in a manner compatible with the case study strategy, by first justifying the use of Strauss’s approach in this integration and secondly showing how this integration might be achieved.

Keywords: Grounded theory, Strauss’s approach, Case study, IS Research Methodology
Résumé

Aucune recherche conceptuelle/théorique en SI n'a encore spécifié comment la théorie enracinée peut être employée comme méthode pour être incorporée dans une stratégie interprétative d'étude de cas, afin de constituer une méthode de recherche. Ce papier est donc écrit pour aider les chercheurs en SI qui souhaitent utiliser la théorie enracinée comme méthode d'analyse des données de manière compatible avec la stratégie d'étude de cas.

Introduction

Grounded theory has been used by many IS researchers since the beginning of the 1990s (see for example Orlikowski 1993; Urquhart 2001; Fernández et al. 2002; Linden and Cybulski 2003; Allan 2003; Sorrentino and Virili 2005; Hansen and Kautz 2005; Coleman and O'Connor 2007). It is becoming increasingly popular in IS research, as there is a widely held belief that it is a reliable method by which to investigate social and organisational phenomena, although it is still relatively new to this field (Jones and Hughes 2004), having been first applied to IS research about thirty years after its development by Glaser and Strauss in 1967.

The general goal of grounded theory is to generate theories derived from data in order to understand the social context. It is a “qualitative research method that uses a systematic set of procedures to develop an inductively derived grounded theory about a phenomenon” (Strauss 1990, p.24). Hekkala (2007) indicates that grounded theory has been used in IS research as a method (by, among others, Urquhart 2002; Jones and Hughes 2004) but that it has also been sometimes used as a methodology (by researchers including Orlikowski 1993; Goulding 1999; Goede and Villiers 2003). Hekkala (2007) states that those who use it either as method or as a methodology do not soundly and logically demonstrate and justify their use of this theory for either of those purposes. The current authors define method as a procedure or technique used to collect and/or analyze data, whilst a methodology refers to the entire research process, from the identification of one or more research questions and the selection of a research method through to the formulation of the findings and results, in which the entire process is based on philosophical assumptions (ontology and epistemology). This view of the two terms coincides with Avison and Fitzgerald’s (1995) definitions: a methodology is a collection of procedures, techniques, tools and documentation which is based on some philosophical view; otherwise it is merely a method, like a recipe. A case study method which includes grounded theory analysis under interpretative assumptions would therefore be classed as a methodology. The aim of this paper is to argue that grounded theory (as a method) can be combined with case study method to construct a compatible research methodology, and to highlight how this combination may be achieved.

The rest of this paper comprises six sections. The first of these sections presents the philosophical paradigms of IS research and their influence on method selection. The next section discusses the two approaches to grounded theory, and the third section explains the procedures and techniques of grounded theory as a method for data analysis. The fourth section justifies the reasons for using grounded theory (Strauss’s approach) in combination with case study method to construct a methodology emerging from this integration, while the fifth section shows the criteria for evaluating the proposed methodology and presents the roadmap, including all the methods and techniques, covering every stage of the research. The final section provides a summary and conclusion. In this paper, the authors draw upon their personal research experience when combining grounded theory and case study method gained during the investigations into the factors influencing IT adoption. It is important to note that this paper does not explain what a case study research is because it assumes the reader’s knowledge of this method (see for example Yin 1994; Walsham 1995).

IS Research Paradigms and associated Research Methods

Klein & Myers (1999) distinguish three paradigms of IS research: positivist, interpretive, and critical. These paradigms are different according to the philosophical assumptions of whether the empirical world (ontology) is considered to be objective and exist independently of humans, or is subjective and constructed through human action and beliefs. Also, there are assumptions about the nature of knowledge (epistemology), how it is created and evaluated.

Positivist research considers the social world exists independently of human action and beliefs and can be described by measurable variables, which are independent of the researcher and human action and experience (Orlikowski & Baroudi 1991). It is concerned with testing theories in order to predict and discover facts and laws. Interpretative
research considers that the world is constructed and interpreted by the human actions and beliefs and that the main aim of interpretative research is to understand the phenomena and make sense of the research problem through accessing the meanings that are assigned by the human (Orlikowski & Baroudi 1991). Interpretive research considers that scientific knowledge is not captured in hypothetical deductions but through the understanding of the human and social interactions by which the subjective meaning of the reality is constructed (Walsham 1995). Critical researchers believe that social reality is historically constructed and that it is formed and reformed by people (Myers and Avison, 2002). The basic difference between critical and interpretive research is that the former is transformative in its nature, focusing on changing the status quo (e.g. "related to emancipation and empowerment"), while interpretive research can be seen as more neutral and descriptive (Khazanchi & Munkvold 2003). Klein and Myers (1999, p.3), state "IS research can be classified as critical if the main task is seen as being one of social critique, whereby the restrictive and alienating conditions of the status quo are brought to light".

Research methods are usually classified into quantitative and qualitative. Grounded theory, case study, ethnography and action research are qualitative research methods that are typically associated with interpretive paradigms. However, a case study as a qualitative research method can be either positivist or interpretive (Myers & Avison 2002). For example, if a case study is planned to focus on exploring the implementation of IT strategy within a particular organization, where the role of the researcher is solely to test and seek answers to predefined and fixed questions (i.e., there is no change of questions in response to the answers provided by the participants, even if the answers vary in reflection of the individual’s particular experiences and beliefs), then this case study is based on positivist assumptions and not the interpretive assumptions that are typically associated with case study method application. Therefore, it is crucial when integrating two or methods, such as that proposed within this paper with respect to case study and grounded theory) to make sure that the philosophical assumptions behind the methods are the same.

Grounded theory variants

Grounded theory was developed by Glaser and Strauss (1967), and their combined work can be considered as the first version of this theory. Strauss and Corbin (1990, 1998) subsequently developed and extended the original theory, which later faced criticisms from Glaser (1994). The divergence between the two original authors leads to what is commonly termed the Glaserian approach and the Straussian approach to grounded theory (Hekkala 2007).

In the IS field, many researchers have applied grounded theory without even mentioning that there are two distinct approaches. Hekkala (2007) confirms this by giving examples of papers (see for example Orlikowski 1993;; Galal and McDonnel 1997; Lubbe and Remenyi 1999; Lehmann 2001; Rowlands 2005) where there is no mention as to the variant of grounded theory being adopted. Thus, identifying the attributes of the two approaches is essential to help researchers be aware from the outset as to which approach is more appropriate to their research and to adopt with case study research. Onions (2006) highlights the major differences between the two grounded theory approaches as shown in Table 1.

<table>
<thead>
<tr>
<th>Table 1. Grounded Theory Variants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Glaserian Approach</td>
</tr>
<tr>
<td>Beginning with general wonderment (an empty mind)</td>
</tr>
<tr>
<td>Emerging theory, with neutral questions</td>
</tr>
<tr>
<td>Development of a conceptual theory (abstraction of time, people and place)</td>
</tr>
<tr>
<td>The theory is grounded in the data</td>
</tr>
<tr>
<td>Inductive method</td>
</tr>
<tr>
<td>The researcher is passive, exhibiting disciplined restraint</td>
</tr>
<tr>
<td>Data reveals the theory</td>
</tr>
<tr>
<td>Coding is less rigorous, a constant comparison of</td>
</tr>
</tbody>
</table>
incident to incident, with neutral questions and

categories and properties evolving. Take care not to

'over-conceptualise', identify key points

| The nature of making comparisons varies with the
coding technique. Labels are carefully crafted at
the time. Codes are derived from 'micro-analysis
which consists of analysis data word-by-word'

| Two coding phases or types, simple (fracture the
data then conceptually group it) and substantive (open
or selective, to produce categories and properties)

| Three types of coding, open (identifying, naming,
categorising and describing phenomena), axial (the
process of relating codes to each other) and
selective (choosing a core category and relating
other categories to that)

| Regarded by some as the only 'true' Grounded Theory
Methodology (GTM)

| Regarded by some as a form of qualitative data
analysis (QDA)

The role of existing literature within research activities is clearly different between the two approaches. Specifically, Glaser (1992) asserts that the literature should not be examined before commencing the study so as to avoid constructing prior assumptions and beliefs which might unconsciously bias the researcher. He says "there is a need not to review any of the literature in the substantive area under study" (Glaser 1992, p. 31). He continues (Glaser 2004, p.9) that the "pre-study literature review of QDA [Qualitative Data Analysis] is a waste of time and a derailing of relevance for the GT [Grounded Theory] Study". Glaser (1992) supposes that the research problem and questions are only discovered once coding begins and "the research question in a grounded theory study is not a statement that identifies the phenomenon to be studied" (p.25).

In contrast, Strauss and Corbin (1990) acknowledge that there should be some survey of the literature before the fieldwork commences and that the researcher enters the research area with some knowledge of the phenomenon being studied. Strauss and Corbin (1990) believe that the literature can be used to derive questions that the researcher desires to use in field work. They state that "The research question in a grounded theory........ tells you what you specifically want to focus on and what you want to know about this subject" (Strauss and Corbin 1990, p.38). They also state that the literature directs the theoretical sampling, and is helpful for theoretical sensitivity (see later sections for definition of these terms). Furthermore, it can be used as way for supplementary validation, meaning that after the researchers finish their research, they could show how it differs from previous literature or includes common findings.

Hekkala (2007) states that the Straussian approach is an inductive-deductive one; deductive as the researcher has some preconceived theories and hypothesis, and inductive as it enables new concepts to emerge. Surveying the existing literature is necessary in order to help the researchers identify the relevant concepts and theories of their research. It lets the researcher make sense of data that is gathered from the fieldwork.

Glaser (2002) criticises the Straussian approach, stating that he is forcing a theory from the data because he forces data into predetermined paradigm model (i.e., cause, condition, context, and consequence) relationships rather than letting any theory emerge. In the Glaserian approach the researcher does not have to find preconceived causes, consequences or action/interaction relationships (Glaser, 1992). According to him this paradigm model is the aim of qualitative data analysis, termed by him to be a "full conceptual description". For this reason, as stated by Hekkala (2007), Glaser claims that Strauss and Corbins' (1990) approach can only be considered as a method providing techniques for data analysis, not a methodology. Glaser (2004) states that the original version of grounded theory (Glaser and Strauss 1967) is a methodology while the later versions are QDAs. Glaser (1992, 2002) maintains that the Straussian approach focuses on conceptual description by spending time describing the researched situation and categories without abstracting the time, people and place, while the original or classical grounded theory, as he likes to name it (Glaser 2004), focuses on conceptual analysis by concentrating on conceptualisation and abstraction of data, and generates conceptual hypotheses that can be applied to any relevant times, places and people. However, Strauss and Corbin (1990) also claim that the researcher whose uses grounded theory should analytically move from description to conceptualisation in the selective coding stage.
Grounded theory procedures

This section elaborates on Strauss's procedures of analysis in order to show subsequently how these can be combined with the case study research method to form a viable research methodology. Hekkala (2007) notes that most IS researchers rely on Strauss and Corbin's (1990) book, which concentrates on providing techniques for researchers who want to use grounded theory.

Strauss and Corbin (1990) assert that the coding procedures in grounded theory are neither automatic nor algorithmic - "we do not at all wish to imply rigid adherence to them" (Strauss and Corbin 1990, p.59). In other words, flexibility may be necessary in certain circumstances.

Coding is the key process in grounded theory (Strauss and Corbin 1990). It begins in the early stages after the first interviews for data collection. This process comprises three coding steps. Through this process, two analytical techniques are used. The first is constant comparative analysis, which is a continuous process of identifying conceptual categories and their properties emerging from data by consistent comparison of that data. The researcher needs to be sensitive, which means the ability both to identify what data is significant and to assign it a meaning. This sensitivity comes from experience, especially if the researcher is familiar with the subject under investigation. The literature review is another source of the theoretical sensitivity (Strauss and Corbin 1990), and so are the expressions of the interviewees themselves, in particular when they repeat the same phrases and concepts. The other technique is the asking of questions. Once the researcher names the concept (event, idea, action and incident) then he or she asks questions regarding such things as what this is and what it represents.

The three steps of coding are:

Open coding is "the process of breaking down, examining, comparing, conceptualizing and categorizing data" (Strauss and Corbin 1990, p.61) by which concepts and their proprieties and dimensions are identified from data that are transcribed by the researchers. This can be achieved either line by line or by focusing on main ideas in sentences or paragraphs (Strauss and Corbin 1990). Each code represents a word or sentence containing a meaningful idea, and a group of codes (two or more) forms a concept. A concept is an abstract representation of an event, object or action. In open coding, events, objects and actions are compared with others in terms of similarities and differences in order to give them, when similar, the same name. The name or label that is assigned for a category should be selected logically and usually seems to represent the data and be related to it. A reading of the literature gives the researcher an initial set of concepts that can be used, but researchers should not be constrained by these concepts; rather they should focus on the words and phrases used by the participants themselves. It is in this way that names are assigned to categories (Strauss and Corbin 1990).

Axial coding is the process of reassembling data that were broken down through open coding. Essentially, it is the process of relating categories to subcategories. Categories are higher in level and more abstract than concepts, and are generated by constant comparison of the similarities and differences between such concepts. This is done by using what is called the 'paradigm model', which enables the researcher to think systematically about the data and relate them to each other. This model addresses the relationships between the categories by considering the following aspects:

- **Causal conditions** represent incidents or events that lead to the occurrence of the phenomenon.
- **Phenomenon** represents the central idea or event, indicate about which a set of actions/interactions are directed at meaning or handling or to what extent that the set of actions are related.
- **Context** refers to specific properties related to a phenomenon. It represents a set of conditions where in which action/interaction strategies are taken.
- **Intervening conditions** can exercise influence by facilitating or constraining the action /interaction strategies within a particular context.
- **Action/interaction strategies** are devised to manage, handle, carry out and respond to a phenomenon under a specific set of conditions.
- **Consequences** are the outcomes of action and interaction.
**Selective coding** is the process of integrating and refining the theory. The first step in integration is to identify the central or core category, which represents the main theme of the research. To be core, the concept must appear repeatedly in the data. The central category acts as a master that pulls the other categories together to form an explanatory “whole picture” by using the paradigm model. In this step the categories are refined at a high level of abstraction, and categories that need further explication are given more descriptive details (Strauss and Corbin 1990). The integration is not dissimilar to axial coding except that it is done at a higher, more abstract level of analysis, and the subcategories are linked to the core category. Finally, a story line which is a conceptualisation of a narrative description of the study's central phenomenon is analytically explained.

In summary, the following sequence is followed in grounded theory in order to arrive at the research model (theory) which is grounded from the data:

Codes → Concept(s) → Categories → Model (Theory).

Sampling in grounded theory is based on theoretical sampling, on the basis of concepts that have been shown to have theoretical relevance to the developing theory. It is related to the sampling of new data based on the analysis of that initially collected from the previous interviews, where the concepts that emerge constantly guide the researcher as to the nature of future data, their sources and the issues to be discussed in subsequent interviews in order to develop the categories. The initial questions for the fieldwork are based on concepts derived from literature (i.e. data gathered previously), which provides the researcher with a starting point and a focus; later, the sampling becomes more in-depth. Strauss and Corbin (1990) explain that the sampling should focus on sampling incidents and not persons per se – in other words, collecting data about what informants do or not in terms of action/interaction, condition and consequence of the action. The researcher continues this process until the theoretical base is saturated, where no new data emerges regarding categories and their relationships.

**Justification for using grounded theory and in particular the Straussian approach with case study method**

Fernández et al. (2002) state that grounded theory (the Glaserian approach) and case studies can be used in combination. Fernández et al. (2002) adopt a Glaserian approach with this combination. However, this appears incongruous as the use of this approach means that the researcher should not review any literature before the fieldwork, and that the research question is based on the emergence of codes during data collection and analysis – yet this is contradictory to the case study research that was developed by Yin (1994).

Hughes and Jones (2003) state that grounded theory is consistent with interpretive case studies that investigate social and organizational contexts. Hughes and Jones (2003) suppose that there are some justifiable reasons for the use of grounded theory in interpretive case studies. Nevertheless, they do not show how and why the case study is consistent with grounded theory and could therefore be combined to form a methodology, and which variant of grounded theory is more appropriate.

Hughes and Jones (2003) also state that empirical work shows a discrepancy between the interpretive perspective and the grounded theory procedures by which they ought to be applied, where the procedures of coding, comparing, categorizing and saturating have a positivist and mechanistic attitude. However, Strauss and Corbin (1990) defend their position, stating that the procedures used in grounded theory are neither automatic nor algorithmic, and that they do not compel the researcher to adhere completely to them. Furthermore, by using the techniques of constant comparative analysis and of asking questions for each code (i.e. what does this mean and what does it represent), interpretations are made by the researcher, especially when new concepts emerge; this is still under the interpretative assumption that the researcher is considered part of the research process.

Pandit (1996) proposed a framework that he adopted in his doctoral study for building theory which was dependent on Strauss and Corbin (1990)'s grounded theory variant and which incorporated some elements of the case study research method. This framework demonstrates the procedures from defining the research question until building the theory and ending by comparing the resulted theory with the literature. However, whilst this framework provided useful guidelines for building the theory, and whilst the framework has some identical procedures to that defined in the proposed methodology in the present paper, his paper does not provide answers as to why the Straussian approach, and not the Glaserian one, can be integrated with case study research. The aim of the present paper is to justify that case study and grounded theory as a method can be compatible, but only if the Straussian approach is used.
In essence, there is a similarity between the case study method and the Straussian approach to grounded theory, as explained below:

- The case study strategy devised by Yin (1994) suggests that the researcher should start with a specified problem statement and a set of research questions and propositions. He states that research propositions direct the researcher to focus on what kinds of information to collect; with no research propositions the researcher might be tempted to collect everything. These propositions emerge from existing literature. He furthermore refers to the literature review in order to develop the case study protocol which includes the research objectives and case study questions that are used as a reminder rather than as the actual questions by which data is collected from the interviewees. Identifying previous constructs guide the researcher to form the preliminary design of theory-building and serve to evaluate them accurately in interviews (Eisenhardt 1989). Eisenhardt (1989) states that it is important for researchers to recognize that it is impossible even in the case of theory-building research to start with a clean theoretical base, but that researchers should predetermine prior variables without finding relationships between them. They should also not be restricted by only those as sometimes new factors are found during data collection that need to be added and reform the theory. This also agrees with Strauss and Corbin’s (1990) approach that the researcher cannot start without any literature on the phenomenon that is being studied; nevertheless, the researcher is not limited by the literature and embraces the flexibility of accepting emergent ideas. Moreover, the research question in grounded theory should tell the researcher specifically what to focus on and what the researcher wants to know about the subject of research.

- Both case study and grounded theory using interviews as a technique for data collection (Allan, 2003), and both consider the interview to be the main source of data (Yin 1994; Walsham 1995; Strauss and Corbin 1990).

- The chief characteristic of case study research is the specification of the boundary and the scope of the research cases and the unit of analysis (e.g. organization, group of people, certain system, activity); this is compatible with the grounded theory concept of theoretical sampling as mentioned by Strauss and Corbin (1990) where the criterion for selection of the cases and the unit of analysis in the case study is relevance, and theoretical sampling serves to seek in-depth information from the cases, and to discover and develop the concepts and theories.

- The generalization of research findings by case study and grounded theory is similar in that the results of the research might be transferred to another context and situation with similar characteristics. Grounded theory aims to develop theories and concepts that can be generalized and applied to other situations. The generalizability of the grounded theory is partly achieved through a process of abstraction; the more abstract the concepts, the more theory applicability (Strauss and Corbin 1990). In the same way, Yin (1994) states that in case study research the researcher’s aim is to expand and generalize theories: “analytic generalization” rather than “statistical generalization”. Walsham (1995) specified this analytical generalization by the developing of concepts, the extending and generating of concepts and theories, and the drawing out of specific implications.

It can be said that the major difference between the case study and grounded theory is that the latter details the procedure of data analysis as discussed in the previous section, while the analysis process proposed by Yin (1994) including pattern matching and explanation building is not as rigorous for analyzing an interpretive case study data as the procedures and techniques provided by Strauss and Corbin (1990); including coding steps, constant comparative analysis and theoretical sensitivity and sampling. One of the main criticisms of the case study is related to the analysis of huge qualitative data where there is no standard analysis approach (Darke et al. 1998). Therefore, this justifies the need for systematic procedures for analyzing data collected from case studies, where, in this paper, the grounded theory (i.e. Straussian approach) is integrated with the case study to fulfill this purpose.

One of the issues that may emerge regarding this combination is whether there are any differences between integrating a single case study with grounded theory and integrating multiple case studies with grounded theory. Yin (1994) states that the case study can be single either if it is unique or revelatory, or if it represents a critical case for testing a well-formulated theory. Walsham (1995) states that a single case study allows the in-depth investigation of the phenomenon and the collect of a rich description. Benbasat et al. (1987) also states that a multiple case study is good when the aim is to describe some entity from different perspectives, to build theory, and/or to perform cross case analyses and comparisons which ultimately lead to more general research results. The present authors believe that the way of analyzing data under the proposed case study and grounded theory integration is similar regardless of the number of cases. However, in terms of theory constructing and richness, as the number of cases investigated and analyzed grows (Eisenhardt 1998) suggested that the number of cases from four to ten is desirable for theory building using case study research), the theory may become more coherent and more able to cover variant situations. If a comparison between cases is the intent then the unit of analysis within each case should remain identical, as
Research Methods

should the procedures of analysis. Furthermore, constant comparative analysis between segments of data continues
to apply to data irrespective of whether that data has been gathered from case number one or case number n.

Evaluation of the proposed methodology

Yin (1994) has proposed a set of tests and criteria (validity and reliability) for evaluating the quality of a case study.
Strauss and Corbin (1990) also define a set of criteria and a group of questions in order to ensure that concepts,
categories and theories are fully developed and grounded. Yin's (1994) criteria are not adopted in this paper for
evaluating the proposed methodology, which combines case study and grounded theory, because these criteria are
measures only suitable for positivist quantitative research, and are not for interpretative qualitative research
(Golafshani 2003). Whereas positivist quantitative research aims to test and predict hypotheses, interpretive research
aims to understand the phenomenon within its natural setting and the human insight. Thus, the criteria for evaluating
the positivist view are not appropriate for the interpretative, since the aim of each one is different. On the other hand,
Strauss' criteria could form the basis of the evaluation in particular of generated concepts and theory. Because both
case study and grounded theory are integrated under the umbrella of interpretative qualitative research, the
combination of both as a methodology involves finding a mutual basis on which to evaluate that methodology. This
is why Lincoln and Guba's (1985) criteria are adopted: they are designed for interpretative qualitative research in
general, and their criteria evaluate the entire research process. These criteria are:

• Credibility, which demonstrates that the research was conducted in such way that its subject was correctly
identified. Credibility is enhanced by using multiple sources as evidence for data, by assigning to various
respondents the concepts and meanings that have been gathered in order to find matches, by allowing participants
to check their interview transcripts and give comments on them, by using data triangulation, and through
prolonged engagement in fieldwork.

• Transferability, which shows whether the findings can be generalized to other situations. The generalization in
interpretive qualitative research is not deduction from small samples to large populations, but is rather to show
how certain findings can obtain the same results when they are transferred to other contexts with similar
properties. This can be achieved by providing the reader with rich, detailed information of the context that has
been investigated.

• Dependability, which shows that the research process is systematic and well documented and can be traced, and
which gives documentation of the methods and approaches used in the research.

• Conformability, which assesses whether the findings emerge from the data collected from cases and not from
preconceptions by showing raw data and demonstrating the steps of the analysis leading to extraction of the
results and outcomes.

Interestingly, Pandit's (1996) case study and grounded theory combined methodology is assessed using Yin's
criteria. As argues above, these criteria are not appropriate for interpretive research. In essence, Pandit (1996) did
not distinguish between the IS research paradigms in his framework and consequently provides no
acknowledgement as to whether the case studies in his framework are positivist or interpretative, and of the different
evaluation requirements of each.

Figure 1 illustrates how grounded theory can be integrated with the case study research method to form a research
methodology. As shown in this figure, the researcher starts with a general research topic. In order to identify gaps,
discover new areas of research or extend the existing body of knowledge, the researcher reviews the literature.
Based on this survey, the problem studied becomes more limited and the research's question is identified; this
defines the aim of the research. The survey helps the research identify the relevant concepts and theories pertaining
to the research question, and consequently models or a set of propositions (concepts) are proposed. These are not to
be tested or validated, but rather serve to enhance theoretical sensitivity and sampling. The cases and units of
analysis are selected for their relevance to the research question, and the research protocol is prepared including
research questions to be asked in the field by considering flexibility and enabling new data to emerge. These data are
collected principally from interviews, but possibly also from documents, observations and artefacts. In fieldwork,
the interplay between data collection and analysis is processed simultaneously by identifying ideas emerging from
the first interviews, so that the area under study becomes more focused as time progresses. At the same time
theoretical sensitivity and sampling and constant comparison between data are taken into account finally result in
that data becoming saturated, which is the point at which no new ideas emerge. A systematic process of coding
begins once the empirical data has been gathered, at each step of which there are outcomes: codes and concepts, and
categories and relationships between them. These ultimately form the research model. It could be that the resulting categories and relationships are not fully saturated, so a second round of data collection and analysis is initiated, which develop new version of the research model. The entire process that results in this model is then evaluated according to criteria of credibility, transferability, dependability and conformability. Finally, the researcher may show the originality and the contribution to the literature by comparing the present research with the previous work and the initial model.

Conclusion

This paper provides contribution in two ways: firstly, for all IS researchers, this paper has provided theoretical development in methodology. In particular, it has justified the use of Strauss' approach to grounded theory in conjunction with case study research, under interpretive assumptions, as a methodology. The paper clearly distinguishes the proposed methodology from that of Pandit (1996), as well as providing the way of evaluating the methodology, and examining the implications for the proposed road map should the case study be single or multiple in nature. Secondly, for beginner researchers in the field of IS, it provides them with the main issues that they will need to understand if they want to use grounded theory as a method with a case study research, by showing how the elements of case study and grounded theory are compatible. The current researchers have adopted this methodology for conducting empirical research and this provides some evidence as to the methodology’s effectiveness.
Figure 1. Case study-Grounded theory Methodology
Halaweh et al. / Integrating the Grounded Theory and Case study Research

References


Onions, P. “Grounded Theory Applications in Reviewing Knowledge Management Literature”, in postgraduate research conference, Methodological issues and ethical consideration”, Leeds Metropolitan University, UK, May 24th, 2006.

Twenty Ninth International Conference on Information Systems, Paris 2008 11


Security Perception in E-commerce: Conflict between Customer and Organizational Perspectives

Mohanad Halaweh, Christine Fidler
School of Computing
De Montfort University
Leicester, UK
Email: {Mohanad, cf} @dmu.ac.uk

Abstract—Security is one of the principal and continuing concerns that restrict customers and organizations engaging with e-commerce. The aim of this paper is to explore the perception of security in e-commerce B2C and C2C websites from both customer and organisational perspectives. It explores factors that influence customers' perceptions of security. It also highlights conflicts between customer concerns with respect to security and those of an organization; existing research has not highlighted this issue greatly. This research provides a better understanding of customer needs and priorities on the subject of security, and enriches the currently available security perception literature, by providing new insights from empirical research conducted in Jordan. A qualitative research approach was adopted, since the research seeks an understanding of human (i.e., customer and organisational employee) perceptions.

I. INTRODUCTION

Security is the challenge and the main problem for successful e-commerce implementation, as stated by many researchers [1]-[6]. However, there is wide agreement between academic researchers that security is not only a technical challenge; rather it involves managerial, organizational and human dimensions to be more effective [7]-[12]. Therefore, understanding (and acting upon) the customer's perception of security is vital to successful e-commerce interactions, because even when a company uses the best technical solutions that provide full security, without the underlying perception and awareness from customers that their particular website is secure, then these technical solutions may mean nothing. Salisbury [13, p.2] defined security perception as "...the extent to which one believes that the Web is secure for transmitting sensitive information..." (e.g. credit card details), where the meaning of security is subjective and which can therefore vary from one person to the next. The target sample of this research, which seeks to understand security perception from both customer and organisational perspectives, is taken from selected Jordanian organizations and Internet users. The reason for choosing the Jordanian context is both in general and for Jordan in particular. This research will be the first of its nature in Jordan, focusing on security in these applications from both customer and organizational perspectives. It specifically addresses Business-to-Customer (B2C) and Customer-to-Customer (C2C) e-commerce websites.

II. LITERATURE REVIEW

In the literature, most security research that is relevant to e-commerce within the IS domain, focuses either on the organization (including technical implementations), or on the customer. In particular, these studies identify systematic processes and factors that need to be considered when implementing a secure e-commerce application from the organizational perspective [19]-[24]. Other research have investigated customers' perceptions and beliefs about security controls and features in e-commerce [25]-[29]. Little research has been conducted which investigates the customer and the organization jointly as a single phenomenon with respect to e-commerce security. This "holistic" view leads to research insight that enables organizations to use certain security solutions that are wholly aligned with customer's objectives and perceptions, thereby reducing the gap between the technology utilized and solutions implemented by organizations, on the one hand, and that being perceived by customers, on the other.

With the existing literature, several factors have been identified as having influence on the customer's perception of security, such as attitude toward security, user's knowledge and experience of security features, ease of use of the interface and presentation of the website, presence of third party security seals such as Verisign and of third party privacy seals like TRUSTe, presence of SSL encryption as indicated by a small padlock, presence of https in the address bar, presence of a security and privacy policy, and the electronic receipt and acknowledgement of the process [25]-[30].

III. RESEARCH METHOD

A qualitative approach which is suggested by [31] is adopted. Qualitative research is subjective in nature, and involves examining and reflecting on meanings and perceptions of individuals in order to gain an understanding of so-
cial and organizational phenomenon. It assists the researcher in understanding the target phenomenon in depth and in its natural setting. A total of 27 interviews were carried out; 15 with customers, and 12 with organizations' business managers and IT staff. The questions that were used for asking customers were open, and focused on exploring their perception of security and how they would check to see if a certain website was secure or not. On the other hand, the questions posed of organizational staff focused on identifying their perception of, and viewpoint on, customers' concerns of security and what issues customers needed to know for distinguishing between a secure website from a non-secure one. During the presentation of the results that emerged from the fieldwork, the researchers provide several quotations from the interview transcripts (presented in italics during the results narrative), in order to show how the "story" derived from this research is relevant and grounded on the meanings that were assigned by the participants themselves (as understood by the researchers).

IV. RESEARCH FINDINGS

This section presents the findings regarding Jordanian customer e-commerce security perceptions, from both customer and organizational (through the eyes of selected technical and managerial employees) perspectives.

A. The Customer perspective

Customer answers with regard to how to check security of a website and what criteria to consider when doing so can be categorized into those referring to tangible features and those referring to intangible features. Tangible features are technological security features on the website that can be checked by users visiting the website, such as https, padlocks, security certificates and security symbols, while intangible ones are not seen on a website yet the user needs to understand or have knowledge of them. They are affected by society in terms of communication and the environment where the customer lives and what they hear from others, as well as their past experience, such as whether the website is well-known and reputable. The perception of the intangible features is constructed by informal word-of-mouth communication between people.

Tangible features need to be understood and checked by the customer on a website, rather than captured through social discourse between people; understanding is gained by having knowledge and experience of these features: for example, in the case of security certificates, a customer needs to know what it means to have one, and how s/he can check to see if it has expired or not.

Some customers indicated that tangible indicators meant very little to them, and much less that the intangible indicators. When considering Website security, the intangible issues surrounding that website were given priority, and only after these had been considered might the tangible ones be checked. For example, the following participant indicated that the presence of a padlock on a website provides him with an indicator of security, but that he does not rely solely on that indicator; rather, he relies more heavily on other people's experience and commendation of the website (an intangible factor).

In fact this depends on what people say, for example, I heard that the padlock in the bottom of the page means this website is secure... but the main thing for me is what other people say because they have had experiments with these websites before me.

Some respondents indicated that the presence of details about security features on the website and information about website policies, besides the interface design, would make them feel that it is more secure. Examples from the participants' responses are:

I mean sometimes the website provides you information that makes you feel a sense that this website is secure and also through transferring between Internet pages, step by step, until arriving at the confirmation page. This gives me feeling that they are serious and secure.

If the website shows the customer a brief description of what security issues they should be aware of and an understanding, then this makes the customer more trusting of the website.

In fact this depends on what people say, for example, I heard that the padlock in the bottom of the page means this website is secure... but the main thing for me is what other people say because they have had experiments with these websites before me.

Some respondents indicated that the presence of details about security features on the website and information about website policies, besides the interface design, would make them feel that it is more secure. Examples from the participants' responses are:

I mean sometimes the website provides you information that makes you feel a sense that this website is secure and also through transferring between Internet pages, step by step, until arriving at the confirmation page. This gives me feeling that they are serious and secure.

If the website shows the customer a brief description of what security issues they should be aware of and an understanding, then this makes the customer more trusting of the website.

I read their policy and all information that was relevant to the website if I have doubts about this website...

Participants reported that the availability of a third party, who is neutral and international, can act as an intermediary and be accepted by all parties, thereby guaranteeing that security is provided, making them perceive that a website is secure and consequently enabling their engagement in e-commerce. For example, one participant suggested:
A few participants highlighted the significance of the website’s existing known (and typically physical) identity, such as that of the banks and telecommunications companies in Jordan; participants appear not to use websites which are anonymous and have no real physical location:

I trust only the bank .... Suppose if anything happens then I can go to them and refer to them since they have a physical place.

In fact, I was a customer of this bank for long time so I discarded the fact that the bank would steal or trick me. But there are some instructions, I should know them as a customer to protect myself from any person. For example, the first time when I logged onto the system (website page) it forced me to change the password after six months. I did that but later on I tried to enter it... I forgot the new password I tried many times and then the system asked me to contact my branch to activate my password, because I entered the incorrect password more than three times...... all of these processes are in order to protect me so they are very concerned on security.

The last quotation also showed that, from this participant’s perspective, the security of his online account is addressed by providing a strong password procedure. This reinforced his perception that the bank is working to provide on-line security for its customers.

Some participants reported that the characteristics of the company (e.g. respected and large size) would lead them to feel that it supports and provides secure website access.

The company that respects its customers, is well known and especially larger ones, implicitly provides the required conditions in order to complete the transaction in secure way.

One of the participants has not yet bought online but in his opinion there are definitely secure websites. He stated:

I hear that there are many people purchasing over the internet and some people buy and sell shares as well, so certainly it is secure as there are people doing it. otherwise why do they buy and sell if it is not secure.

Table I summarizes all the tangible and intangible indicators of security from a customer’s viewpoint that were derived from the fieldwork, many of which have been touched upon within the preceding discussion (others were not discussed due to paper length limitations, and those that were provide more sufficient evidence of the process of research narrative development). On close inspection, it may appear that several of the intangible indicators appear to be identical: for example, famous, well-known and recognized could be considered to be synonyms. However, the researcher has kept to the customer’s exact phrases rather than presenting (and thereby enforcing) his own interpretation of the words used.
have a generally negative attitude towards online shopping, especially in the Arabic countries. For example, one participant believed that customers nowadays are more aware and have greater propensity to accept online trading given their experiences of using ATMs and the generally wider availability of credit cards. We applied an electronic ticketing system on our website which was an important factor in enabling our business, as a result it has become easy for customers to book a ticket and pay online from anywhere... people are accepting that they are ready more than you think, there was minor rejection but in general it was accepted smoothly by our customers... really, we are surprised how people are ready to accept it...... Customers nowadays become used to an ATM and it is not a big deal, most of people have a credit card... people are more developed than in previous years.

She asserted that her company focuses on strong customer support to allay and respond to customer concerns, by saying:

The customer viewpoint is considered and we have a customer service centre that is responsible for customer’s enquires, claims and problems, and we take on their feedback which is important for us.

Another participant pointed out how his company’s concern was about the customer in respect of the website design. Here, the respondent correlated ease of use in the website with a feeling of security, but immediately went on to say that this, in itself, is not really security.

The user’s viewpoint is necessary for us, providing a website that is easy to deal with, friendly, motivates the customer to use it, which makes him feel it is secure to some extent... but not exactly secure.

The next participant showed how his company considers the customer viewpoint, and what it does to provide secure online transactions. In his viewpoint, a simple and true (i.e., product exactly matches what the customer expects) transaction with the customer makes him/her feel that the website is secure, and this makes the customer experiment and eventually become a repeat user of the website.

In fact, and by my experience with an e-commerce website for several months, I arrived at an unbelievable fact that Jordanian citizens and Arabic customers in general don’t believe or trust shopping online, they think no transparency is provided by the websites. For example traditionally, when the customer buys a computer from a store, he faces a problem if he wants to fix his computer, he is countered with violation of the deal by the merchant, and he is always the weakest party and will ultimately carry the cost of fixing the produce. So, how do we persuade the customer buying online that whilst he does not see anything tangible in front of him, and is not able to touch it with his hands, where he already had faced problems with a physical store... he needs guarantees... really, where the detailed information that is provided by the first page on the website is not sufficient to convince him... briefly, the trust between the customer and merchant is nonexistent as it is not between the customer and Arabic governments.

### Table II.

<table>
<thead>
<tr>
<th>Security features in e-commerce website</th>
<th>Categorizing of security features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Padlock</td>
<td>Tangible</td>
</tr>
<tr>
<td>Security certificate</td>
<td>Tangible</td>
</tr>
<tr>
<td>Transferring between interfaces of the website</td>
<td>Tangible</td>
</tr>
<tr>
<td>Website presentation</td>
<td>Tangible</td>
</tr>
<tr>
<td>Security policy</td>
<td>Tangible</td>
</tr>
<tr>
<td>Acknowledgment via email</td>
<td>Tangible</td>
</tr>
<tr>
<td>Third party symbols</td>
<td>Tangible</td>
</tr>
<tr>
<td>Physical address, telephone # and email</td>
<td>Tangible</td>
</tr>
<tr>
<td>Brief description of the security issues that the customer should be aware of on the website</td>
<td>Tangible</td>
</tr>
<tr>
<td>Known identity (company has physical building, i.e., Bank)</td>
<td>Intangible</td>
</tr>
<tr>
<td>Support password system</td>
<td>Tangible</td>
</tr>
<tr>
<td>Well-known electronic payment gateway such as PayPal</td>
<td>Tangible-Intangible</td>
</tr>
<tr>
<td>Famous brand/company</td>
<td>Intangible</td>
</tr>
<tr>
<td>International</td>
<td>Intangible</td>
</tr>
<tr>
<td>Recognized</td>
<td>Intangible</td>
</tr>
<tr>
<td>Trusted</td>
<td>Intangible</td>
</tr>
<tr>
<td>Well-known</td>
<td>Intangible</td>
</tr>
<tr>
<td>Formal website</td>
<td>Intangible</td>
</tr>
<tr>
<td>Respected company, large size</td>
<td>Intangible</td>
</tr>
<tr>
<td>Reputable</td>
<td>Intangible</td>
</tr>
<tr>
<td>Well-rated</td>
<td>Intangible</td>
</tr>
</tbody>
</table>

B. The organizational perspective

Some respondents indicted their impression in general about a customer’s acceptance and engagement in e-commerce. For example, one participant believed that customers have a generally negative attitude towards online shopping, and that there is no trust and transparency between the customer and merchant:

In fact, and by my experience with an e-commerce website for several months, I arrived at an unbelievable fact that Jordanian citizens and Arabic customers in general don’t believe or trust shopping online, they think no transparency is provided by the websites. For example traditionally, when the customer buys a computer from a store, he faces a problem if he wants to fix his computer, he is countered with violation of the deal by the merchant, and he is always the weakest party and will ultimately carry the cost of fixing the produce. So, how do we persuade the customer buying online that whilst he does not see anything tangible in front of him, and is not able to touch it with his hands, where he already had faced problems with a physical store... he needs guarantees... really, where the detailed information that is provided by the first page on the website is not sufficient to convince him... briefly, the trust between the customer and merchant is nonexistent as it is not between the customer and Arabic governments.
transaction problems, recommend certain sellers and certain products, provide feedback, and request support from the website. In addition, the website provides a rating system which makes customers feel that the website has greater credibility.

One of the important things that makes customers feel that our website is secure and credible is the rating system which indicates positive and negative ranking for buyers and seller, and the best buyers and sellers...... We have a forum on our website and we have seen for example one customer ask a question and another customer tell him to refer to our policy, the clause number#. If the customer faces any problem, we resolve it within 24 hours, the nature of our website is that easy to deal with. It is so that it makes customers feel happy and confident and in control over the work on our website, it is not complicated.

He added that their website is 100% secure and they guide their customers on the first page to check the padlock.

We put on our website ‘secure 100%’, we carry the responsibility for that, there are websites that say that they are secure 100% but they are not secure and just talk rubbish. On our website, we also provide customers with an explanation regarding the security privacy policy

And on that the website, the following instructions are found:

Look for the item with this icon J

This means that the auctions displaying on it are more secure.

In contrast, another participant stated that customer concerns are addressed solely by the services provided on the website:

The customer viewpoint is considered at service level what he would like to see and what he wouldn't like.

Some of the technical staff involved in the development and maintenance of organizational websites did not consider the checking of tangible indicators as a sufficient mechanism for determining the security, or otherwise, of a website. This is firstly because technical staff appeared to be unconvinced that tangible indicators provide real security; websites are hacked despite the presence of these indicators, so customers could be led into a false sense of security by relying solely on them. Secondly, these indicators assure customers of the organization's honesty, for example, by using security certificates as an indicator that the website is guaranteed by a third party, and thus that the website is secure, but this is no assurance that it cannot be breached by hackers.

It is difficult to consider that a website is secure or not even if you are professional, no way to say 100 % secure, and using security certificates just means that you are not lying to your customers by doing your responsi-

bility and this is not a guarantee that you are not hacked by hackers.

These indicators (e.g. security certificate) are thus not sufficient to assure that the website is completely secure. Here, the risk does not come from the website itself but might be from outside parties (e.g. hackers). One participant maintains that there is no way to confirm that their websites are secure or not, even when such websites are very well-known.

Frankly, there is no way to judge that a certain website is secure, even though it is Amazon and eBay.... it is reputation and ease of use, the guarantee is the experiment and reputation.

From the interviews with organizational members, it was also found that naïve customers are sometimes not aware of technological details, such as the meaning of terms like https. Examples from participants reported that security understanding is not an important thing for the customer and that the only concern is others people’s experiences or reputation of the website.

Some people don't care about security, they don't think is it secure or not, they are just concerned about what other people say if it is well know-company and credible by others, then they use it and trust it.

To say this website is secure 100 % means noting for the customer, I think the reputation of the website makes the customer feel it is secure.

The main concern for users is the reputation of the company, they are looking for a well-known company, and people here in Jordan deal with national companies like telecommunications because they know them well.

Thus, from an organizational perspective, customers look for intangible indicators such as reputation, a well known company, and the system of rating by previous customers of the website, in order to assess whether or not a website is sufficiently trustworthy to engage with, regarding online purchases.

V. DISCUSSION

Based on the findings in the previous section, conflict between the some of the views of organizations (in the eyes of management and technical personnel) as to what customers consider important, and those views of the customers themselves, can be clearly seen. The research findings showed that some of the participating organizations indicated their acknowledgement of customer security concerns by stating them on the first page of the website that it was 100% secure. One participant stated that their website then guides customers to check whether a padlock symbol appears when a transaction is performed, advising them that if it does then the website is secure. This raises the question of whether such advice is sufficient to convince a customer purchasing online or performing online transactions. In essence, while it
is important, it may indeed not be sufficient; a responsible company should explain website security to its customers, not merely present a logo or use a short sentence to state that it is secure. Rather, they need to make clear what the padlock means, what technology is used to encrypt the data and what protocols are applied. One participant from an organization pointed out that customers' concerns are considered at the service level, and this should be accepted as a premise and therefore it should be considered that customers are only concerned with the quality of the service provided on the website and whether it is easy to operate. In essence, this can be refuted by the argument that some users know the meaning of security indicators on websites, so that in this context, new thoughts are required; a change of attitude is needed among technical staff, because they tend to underestimate customers' perceptions and their ability to understand what is involved. Thus, organizations exempt themselves from fulfilling their responsibility to educate their customers in issues related to security.

On the other hand, customers' responses have revealed that they do not intensively check tangible security features, being more interested in knowing the identity of the other party; they want to know whether they are dealing with a national company which is well-known, famous and reputable, which are intangible features. If these questions are answered affirmatively, then the customer feels secure. For such customers, security is guaranteed on the basis of the abovementioned features. Consequently, more effort is required by the organizations in this field, namely, to seek strategies to make their websites better known and to boost their reputation. For example, if a customer wants to buy something from Amazon, then does he check whether the site is secure or not? This example would suggest that tangible security features on the website are not essential, but that the customer will decide to buy from the website without checking, simply because he depends on the reputation of this website - and in this case the reputation of the company implies by default that the website provides the required security. This raises another question: does every company which has a good reputation actually guarantee the security of its website? In essence, it can do so only if the company is responsible for the protection of the customer's data from its actions. For example, if a company's website applies the best technology for encryption of customer's data, but then their private data is transferred by the website to another party without the customer's consent, then the violation of security (i.e. confidentiality/privacy requirement) has come from the website itself, despite its supposed reputability; so, the responsibility of the company for security should have two dimensions: protection of data from hackers, and from misuse by the parent organization of the website itself.

Organisational staff indicated that tangible features do not totally guarantee security. The consideration addressed by organisational staff, that there is no way to judge whether a website is secure or not, leads to a reasonable enquiry: if there are no dependable criteria for distinguishing a secure site from an insecure one, what should the customer depend on when purchasing online securely? The justification for this doubt is that while security features (e.g. using SSL, security certificates) of the website may mean that its operator has an honest stance towards its customers, that while their data is encrypted for transmission, that the website's identity is authenticated by a third party and that this, as reported by one participant, means that they do not deceive their customers, and that while the website undertakes to provide secure transactions, none of this means that the company is able to totally guarantee that their site will not be hacked or its security breached. In other words, as another participant stated, it is difficult for even well-known websites to guarantee total security. In essence, this shows how such a significant role is played here by the intangible indicators of security, such as the fame or reputation of the website, which represents the first priority for a customer in deciding whether to buy online. Fame or reputation of the website assures him that the website's operators undertake the responsibility to protect his data. This concurs with the organisation's view that customer concerns are about the reputation of the website, how well known it is, and how it scores on rating schemes, for example. It may be concluded that tangible and intangible security features are both important and need to be checked by customers, who should not depend entirely on one or the other.

Although the core idea of this paper is to investigate security perceptions from the customers' and organisations' perspectives, the researcher has found it is difficult to put some of the participants' responses with respect to trust away, where this terminology was mentioned in their answers. The literature review provides, theoretically and empirically, a set of antecedent factors for trusting e-commerce websites. These factors include the characteristics of the online vendor, third-party certification, the individual's propensity to trust, the influence of perceived risk, perceived security control (i.e. authentication, no-repudiation, confidentiality, privacy concern and data integrity), perceived competence, legal framework, previous experience, perceived credibility, perceived ease of use, perceived privacy, perceived company reputation and willingness to customize products and services, perceived website usefulness, third party recognition, perceived investment, perceived similarity, perceived control, perceived familiarity, and perceived size [32]-[37]. Based on the above, it can be said that perception of security from the customer perspective is determinant on trusting the website, where perceived security is one amongst many other factors that can increase or decrease this trust. Intangible features of security were revealed by the customers, mentioned in Table I., such as reputation, well-known or perceived familiarity of the website, also increase or decrease in belief that whatever certain website is secure or not, even though these features are similar to some of antecedent factors for trust, such as reputation. As a result, this paper extends current literature to show that these factors also influence customer perception of security which is similar to the influence on customers trusting a website.

VI Conclusion

This paper has provided a valuable contribution, by providing insight into the customer's perception of e-commerce security. It has clearly identified that both tangible and intan-
gible features play a major role in the customer perception and judgement of the security of a website. It has highlighted and discussed differences between customer and organizational viewpoints of customer e-commerce security perception, and has delivered guidelines for organizations such as the taking on of the responsibility to educate customers towards security features (e.g. security certificate), what these mean and how to check that the website has these. By taking and achieving this responsibility in protecting customer's data in line with making promotional strategies to make their website more well-known and used, its reputation will increase.

In addition, the paper extends the existing body of knowledge by providing evidence that some factors that influence customer's perception of security are similar to that which makes them trust the website as reported in reviewed literature. Therefore, and to provide sound evidence, this stimulates future research which can address the relation between security and trust, and which can identify, by empirical research, whether the factors that influence customers' security perceptions are the same as those that influence trust (or indeed where they differ). This could be achieved by investigating the perceptions on the two issues together based on the same respondent set.

REFERENCES


ADOPTION OF ELECTRONIC PAYMENT SYSTEMS IN E-COMMERCE WEBSITES WITHIN JORDAN

Mohanad Halaweh, Christine Fidler
School of Computing
De Montfort University
Leicester, UK

ABSTRACT
The aim of this paper is to identify factors that have influence on the provision of Electronic Payment Systems (EPS) on e-commerce websites among Jordanian organizations. Jordan has achieved valuable progress in the IT sector, but with respect to diffusion, full e-commerce is still in its infancy. This paper focuses on the main prerequisite for full e-commerce applications, which is the availability of EPS. Qualitative research was adopted to identify the influencing factors. This also enabled issues to emerge without restriction to any predefined constructs and factors that could be derived from the existing literature. This paper investigated differing perspectives of EPS provision; from the viewpoint of IT solution providers who have recently developed national EPS, from the viewpoint of IT providers who provide a service for the integration of international EPS, and from the viewpoint of businesses that provide electronic payment services on their websites. This enabled the researcher to obtain a wide-range of relevant factors that were considered to influence the adoption of EPS by e-commerce websites in Jordan.

KEYWORDS
E-commerce, electronic payment system, qualitative research.

1. INTRODUCTION
According to Rowley (2000), the development of e-commerce applications can be viewed as undergoing four stages of evolution: the first stage being contact, where the website function is towards marketing and promoting products and publishing content on the website. The second stage, interact, is concerned with exchanging information and communicating with customers, who are searching for information on the website. The third stage, transact, enables financial transactions to take place through ordering/buying via the catalogue, using online payment systems. Finally, the fourth stage, community, is where a two-way partnership between the customer and organization is established, by allowing a customer access to the organization’s database. Currently in Jordan, most organizations have websites to promote their products and services, and by which to contact their customers (Titi, 2005). In other words, they are within the first and second stages of e-commerce development according to Rowley (2000). Electronic Payment Systems (EPS), sometimes collectively termed an electronic payment gateway, are any payment systems that facilitate secure electronic commerce transactions between organizations and users. These include systems such as electronic cash, electronic checks, smart cards and micro-payment solutions such as PayPal (Lim et al., 2007). In Jordan, very few websites have any form of payment system, which is considered to be a principal prerequisite for e-commerce development to move from the second to the third stage of evolution. Al-Qirim (2007) was the first to state that the unavailability of an e-payment gateway in Jordan is one of the key barriers to successful E-commerce. Recently, the PayOne project was developed by STS (Specialized Technical Services) (http://www.sts.com.jo) to provide an electronic payment service for Jordanian governmental institutions, businesses and organizations. Nevertheless, the adoption of EPS is still minimal in Jordan. This research identifies factors that influence EPS adoption in Jordan so that consideration can be given to these factors by organizations to ensure their more effective progress towards full e-commerce.
2. RESEARCH METHOD

A qualitative approach, along the lines suggested by Strauss and Corbin (1990), is adopted in this research. Qualitative research is subjective in nature and involves examining, and reflecting on, meanings in order to gain an understanding of social and organizational phenomena. The use of qualitative research enables the researcher to understand the phenomena in depth, without narrowing their research to certain predetermined variables that require testing. The researcher conducted interviews without reviewing the EPS literature in detail; therefore, the study was inductive in nature, and this assisted in identifying the topic in its current natural setting. It avoided the researcher having to pose direct structured questions and allowed participants to add their own viewpoints and experiences. Subsequent questions were developed and progressed based on the answers to earlier questions. A total of 5 interviews were carried out; two with key participants from business companies that have e-commerce websites, and three from IT provider companies. Examples of quotations are presented in this paper in order to show how the emerged factors are relevant and grounded from data.

3. RESEARCH FINDINGS

Empirical research data confirmed that the provision of EPS is a principal prerequisite for full e-commerce; participants refer to this and the associated problem in Jordan that there are no national EPS. For example, a business manager said:

Do you know that until now, there is no Arabic electronic payment gateway and as you are aware it is difficult trading electronically without electronic payment gateway

Another participant asserted the same point with respect to the unavailability of EPS in Jordan.

One of the challenges we have faced is providing an electronic payment gateway where we should provide our customer secure payment. This web service we got from a USA Company. In fact, there are only one or two companies in Jordan, but they are not strong like these from outside.

The next participant pointed out that the number of business websites who provide full e-commerce, namely an electronic payment service, is very few:

There are few websites that cover full e-commerce solutions such as e-payment services, like those offered by orange and umniah telecommunications companies…. In reality, e-payment technology is applied in small cases …. but this encourages people to challenge risk to pay their cell phone invoice or yearly subscription fees online.

The empirical study also uncovered the following factors that were found to impact and play a major role on EPS adoption: cost issue, the nature of the business that requests the EPS and its target customers, the applied security standards, the ease of dealing with the EPS provider procedures, the ease of dealing with the EPS interface, reputable, popular and well-known EPS to customers and businesses, the availability of EPS on the e-government portal, the cooperative responsibility between different entities, and the interoperability and integration support with various web-based applications in terms of programming languages. The following subsections investigate each of these factors in turn. Each subsection includes the quotations that provide evidence for the factor in question.

3.1 Cost Issues

One of the participants pointed out that the fees and costs that the service or product supplier has to pay for international EPS providers such as PayPal are a financial problem for organizations. Companies like PayPal, who charge fees for each transaction, reduce suppliers’ profits, sometimes to the point where the transaction becomes a loss for the organization.

...As I conduct business online I have to provide payment services on my website by credit cards; visa and mastercard, but in order to perform that you have to connect your website with electronic payment gateway, which provides you the known security over the internet. Here you have to open a merchant account in the USA and then you will enter into a thorny process which appears to never end, and then your money will be transferred to your account after deduction of the commissions for each transaction by the provider. To some degree, you find it is not
profitable. Rather in some cases you pay subscription fees even though there are no transactions taking place on your website.

Another participant said:

...For example, I know that one online auction website in Jordan was closed because the problem was of adding this service to their website. They found it costs them more than they expected, and as you know now, how can they do the process of payment securely if there is no independent financial institution undertaking this activity....

This means that companies who are intent on conducting business online may indeed fail if they do not provide adequately secure EPS. The availability of a lower cost, secure EPS would enable businesses to add e-payments services to their websites and thus support their customer transactions more effectively.

3.2 The Nature of the Business that Request the EPS and its Target Customers

One participant referred to the familiarity of the EPS provider, and that the criteria for selecting a certain EPS provider focused on the popularity and fame of that EPS provider and on security concerns. It also depends on the nature of the business; some businesses have to present an international EPS on the website, which is known to people over the world not only from Jordan. (e.g., as needed on a website that takes bookings from anywhere in the world).

..our business entails dealing with an international and well-known [EPS] provider, one which is accepted from the people’s perspective. This is because our customers, not only from Jordan but also from the rest of the world, know it. ... When we decided to add this facility we evaluated many of the companies that provide EPS and we chose the most popular one, and the most secure one too.

3.3 Security

The availability of EPS is essential in order to perform any online transaction, and security needs to exist to ensure that data is encrypted and protected before the financial transaction proceeds. Before this stage of evolution, security is not an issue, as explained by the following participant:

Well, if you are talking about purchasing and paying over the internet then we should talk about the availability of an electronic payment gateway, but if you are talking about normal websites just for promotions, then it is not necessary to talk about security. Truly, the issue of EPS is still a problem for businesses in Jordan.

The following participant identified security solutions that have been considered by the national EPS:

All Banks registered their card by VbV [Verified by Visa] 3D secure protocol. The general idea of VbV 3D secure is that it’s there to enhance security for using cards online by ensuring the legitimacy of the person and verifying that the person who uses the credit card is the right person who is eligible to use the card, and not someone else, by prompting the user to enter PIN/password information to help reduce fraud.

He continued by pointed out that security standards are applied to provide secure EPS in e-commerce.

Every thing standard is applied in our EPS... SSL, no data stored in the merchant, PKI, Hashing.... We use signed applet ....Java applied to prevent hacking inside the code.... we used PCI compliance .... It is standard use for enhancing online payment data security.

3.4 Ease of Dealing with the EPS Provider Procedures

Many international EPS providers (e.g. Paypal) are well-know internationally and are very secure; however, the problem here is that some providers have complicated rules/procedures and lots of documents to complete before acceptance. For example, one interviewee said that one EPS could not be used to make donations, yet another could manage donations once a guarantor has been found. For example, one participant said:

We ask our client which electronic payment gateway they prefer and we ask them the nature of the product they want to offer on the website, because some electronic payment gateway providers do not accept the payment method. Here, let me tell you something that some of the international payment gateway companies request many documents and their procedure is very complicated.
Another participant confirmed the same notion implicitly when stating:

... Here you have to open a merchant account in the USA and then you will enter into a thorny process which appears to never end...

3.5 Ease of Dealing with the EPS Interface

Some EPS, in particular their interfaces, are difficult to understand and apply. Once the user transfers from the e-commerce website layout to the EPS layout, they are faced with different styles and designs that can cause problems and confuse customers, making them feel that they have lost control of the transaction. This was reported by the following participant:

The choice payment gateway is very important since the end customer wants to interact with an easy to use one and friendly interface without any complexity. Some of them confuse the customer when he moves from the design of the company website to the EPS provider design and some of them involve you registering before you proceed with the transaction.

3.6 Reputable, Popular and Well-Known EPS to Customers and Businesses

E-commerce websites launched from Jordan mostly depend on external EPS providers, such as PayPal and 2checkout, to provide the facility for electronic payments. For this reason, one interviewee indicated that if EPS providers were nationally known, they would be better accepted and adopted in the local community. This suggests that not all local customers and internet users know the available international EPS, whereas a local EPS would be more well-known by the local community and hence more frequently adopted. As the participant said:

We provided our clients 2checkout and PayPal payment service because they have a good reputation, but frankly, these ones don’t make national online purchasing phenomenon at country level, because not many people know these international companies, but providing a payment gateway that is provided by the government can be accepted by people because they trust the government to do everything in order to protect the customer and make public interest.

3.7 Availability of EPS on the e-government Portal

The same participant as mentioned in the previous section pointed out that the main reason for choosing an international EPS was that they tend to have a good reputation. Nevertheless, he suggested the development of a national secure EPS as part of the on-going e-government project. This enables businesses in Jordan to use EPS on their websites similarly to that provided on the e-government portal. This provision would enable business to engage effectively in e-commerce and to perform electronic transactions securely, and with low cost. At the same time, the EPS facility would also increase customer acceptance: citizens would accept an EPS provided by the government because of the general perception of government to be that which provides official and reliable services provision. Payment on certain websites via national secure government payment gateways is considered secure and is guaranteed.

The above comments further indicate that the success of e-commerce in Jordan correlates closely with the success of e-government and the e-government project. The next quotation confirms this previous idea:

I think the usage of E-commerce will be doubled if there is a secure governmental electronic payment gateway similar to that provided for e-government websites.... otherwise E-commerce will not develop and advance.

This is re-iterated by another participant:

We told the government that if it wants e-commerce to succeed then it is not acceptable to perform the transactions in a traditional way... the government should move... we will sign a contract with the government to provide them the EPS for all its divisions.

The concept of conforming appears here, where any revolution or new technology imposed by the government leads people to conform to it. It is debatable whether e-commerce or e-government was established first. Whilst it is known that the e-commerce term came first; the acceptance of people dealing easily and comfortably with e-government services may encourage a popular engagement with e-commerce, especially when on-line payments occur via secure e-government payment gateways. The participant who suggested developing a national EPS with government support, continued by stating the advantages of this action:
This also provides businesses in Jordan with the ability to integrate this web service into their website, where the same electronic payment gateway that is used in E-government website is used itself by businesses. As a result, gaining the favor, approval and creditability from the customer that they are sure it is secure to pay online, will be increased if payment is made via the government, as it can be guaranteed. As a result, this reduces the costs for businesses instead of using international overseas electronic payment gateway which is not accepted or known from the customer side.

### 3.8 Cooperative Responsibility between Different Entities

Another identified factor is the cooperative responsibility between the financial institution and the EPS developer. One participant pointed out to the problem of cooperation between banks. A participant from the national EPS provider stated that developing the EPS system would face some cooperation problems, and there is a need for mutual responsibility to be established between the banks, the government, and the EPS provider:

*We face a cooperation problem with the bank ... they give us low priority.... work can be done within two weeks, takes 6 months, and we spent a long time to connect the server..... We did not face any technical difficulties rather we exported the project outside of Jordan to Dubai and Saudi and others. We host governmental institution and provide online payments where our government still does nothing ...We were ready but the government works slowly.*

The participant also pointed out how the management of banks in Jordan is reticent in making decisions on providing cards for online payment, and how cooperation by banks has evolved over time:

*We started with one bank which releases its card to buy online and the others waited to see the adoption ratio... what happened with the other bank ..... Then the others followed the first one, gradually the 10 banks in Jordan will be connected by PayOne [electronic payment system project] and provide cards for online payment.*

Another problem, present on the new national EPS, is related to the bank's procedures, where cards are only allowed to be used to buy online when the customer requests this facility, as the following participant pointed out:

*In Jordan, there are about 1.5 million credit and debit cards, but the default is that these cards are not accepted in buying items online, unless you ask your bank to add this service....otherwise the card is rejected for payment online.*

The participant added more details on this matter:

*Banks in Jordan add only the cards for purchasing online, based on the request from customers.... Banks do not add this service for all cards because they pay fees for Jordan Visa for each card, so they just provide it based on request. It is free for customers..... now we propose a model for registering all cards to buy items online, but the fees are deducted from the banks by Visa if the customer wants to buy ...the problem here is that the customer should register if he wants to use it online.... This could cause confusion for the customer and here the bank should inform the customer if they want to use the card online they have to register online firstly.... the popup window comes out from the visa page does not make him fear... the easiest scenario is that the bank does this action, not the customer.*

Although some problems are mentioned above, the participant pointed out that Jordan has qualified IT human resources. They developed the national EPS project without technical challenges and this project links e-service websites from outside of Jordan, as the participant said:

*The whole project was developed in Jordan .... We have skilled staff and competencies.... We have two million of investment in this project ... We did not face any technical difficulties; rather we exported the project outside of Jordan ... We host governmental institutions and provide online payments to Dubai and Saudi.*

The new developed national EPS provider claims that the fixed cost per transaction on the national EPS is less than other international EPS providers:

*The merchant pays only a one-time 350 JD fee and we take commission of 4% for each transaction...... we take less than PayPal which takes 5%... if the merchant completes many transactions per day and no fraud cases come from this merchant, then we reduce it to 3%.*
3.9 Interoperability and Integration Support with Various Web-Based Applications

The national EPS provider also refers to the technology used for developing the EPS, which is compatible and integrates with two main familiar development environments, namely Microsoft and Sun:

*We provide the merchant a choice for application on Java or .Net... we have two versions with manuals and the merchant asks the developer to integrate the EPS with his website, and so we support any language wherever the website is hosted.*

4. DISCUSSION AND IMPLICATIONS

After conducting the empirical work and identifying the factors described in the above section, the researcher reviewed the existing literature to see what factors had already been identified as having an impact on EPS adoption. As mentioned previously, this “emergent factors first and existing literature second” approach was undertaken to avoid any bias from previous literature and to allow factors to emerge based on the current situation in Jordan. The literature highlights many factors influencing EPS adoption. For instance, the adoption of EPS involves universal acceptability and cooperation between institutions such as IT providers, businesses, banks and central government (Baddeley, 2004, Lim et al., 2007). Security and trust in the payment system are other primary factors impacting the adoption of EPS (Schwartz, 2001; Chau and Poon, 2003; Yu et al., 2002; Lim et al. 2007). Costs matter (Yu et al., 2002), and the simplicity of dealing with electronic payment solutions in terms of the technology use (Schwartz, 2001; Lim et al., 2007) and the marketing initiatives by the EPS developer to capture the public market attention have also been found to be significant factors in increasing EPS adoption (Lim et al., 2007). Many of the factors identified in the present research match those identified from the existing literature. However, there are four that cannot be found there; the simplicity of the EPS provider procedures, the compatibility of EPS with different technology, the uniformity of EPS for the e-government and e-commerce websites, and the nature of the business and its target customers.

One of the implications from this study is related to security enforcement within e-commerce websites and profits returned. In order to provide a secure channel for online payments, a commercial enterprise has to find an IT provider to integrate their secure EPS with the website, which costs money and so reduces company profits. One participant assessed this loss as being likely to exceed any profit generated, and in this circumstance then it would not be feasible to do business online. The participant stated that if a certain item is sold in a shop for 50 JD, the shopkeeper would expect a profit of 5-10% on the item. However, if he wanted to sell the same item over the internet, then part of that profit would go to pay the EPS provider, and in some cases the whole profit (or even more) might be needed. Thus, the expenditure on secure e-commerce should be less than the profit returned by the company.

In another issue, one participant said that the nature of their business entails using an international payment gateway that is known to all internet users throughout the world, such as payment by PayPal, which is accepted by most people. However, another reported that the international payment gateway does not lead to much purchasing between Jordanian nationals; therefore, there is a need to provide one accepted and known national EPS to Jordanian users. The previous remark highlights the present disparity between the participants’ viewpoint, which comes as a result of researching different target customers from two different businesses.

This research confirms that it is arguable that e-government is a prerequisite for successful e-commerce. and that is a phenomenon which increases the awareness of participation in e-commerce (and not the reverse). In essence, this can be considered correct in certain countries where e-commerce is still in its infancy and where every citizen has to perform routine transactions online, paying bills, tax, and fees online because there is no other way to do this than via the government’s website. If payment is by a national electronic payment gateway that is secure and similar to one provided by the e-government website, then it is more feasible for customers to buy online. Therefore, the success of e-commerce in Jordan correlates with the initial success of e-government, where both are being accepted by customers with positive feelings concerning matters of security and trust.
Although IT solution providers have recently developed a national EPS in Jordan to increase e-commerce adoption there, it needs to overcome obstacles by reducing the business cost of adding this service, providing ways to increase the culture of using a credit card, and making procedures easy for customers to use and understand. There is a marketing role by the IT provider to promote the new national EPS with government support to other organizations, which as yet is not being fulfilled. As one participant stated, “Do you know that until now there has been no Arabic electronic payment gateway...”, yet the gateway has been available for at least one year. The national EPS provider should pay greater attention to this marketing role.

Finally, clear and comprehensive regulations and laws are needed to control e-transactions between parties, as one participant pointed out: “…we want to know if a problem happened between the customer and the merchant... does the judger accept the electronic invoice and can they solve the problem?”

This paper has made valuable contributions. Firstly, it is the first study to focus collectively on Jordan, an EPS and different stakeholder groups, and it has identified factors that influence the adoption of an EPS on e-commerce within Jordan. It has provided decision makers with an insight into these factors, allowing them to set effective strategies to deal with them. For future research, it has provided researchers with a framework of factors that can be investigated further, possibly by examining their impact over a much larger sample of businesses and organizations. The paper has also provided some arguable implications as stated above.

5. CONCLUSION

This research has adopted a qualitative approach to identify and understand the nature of the factors that influence in EPS adoption in Jordan. Jordan is continuing to make developments in the IT sector, and has qualified skilled IT people who are able to develop and export IT products and services to outside Jordan (i.e.EPS). However, these developments involve effective use and acceptance between Jordanian organizations and businesses towards increasing the adoption of the national EPS as an alternative to international ones. In essence, there is a promotional responsibility by the EPS provider in two directions: the first is setting strategies for encouraging the business and organizations that have not yet added the EPS onto their websites. The second direction is for businesses and organizations that already have EPS on their website. In this case, the EPS provider should provide a competitive advantage over the available international payment gateways, such as a lower cost than those from outside Jordan, showing for them that the best security solutions are applied and the simplicity of procedures and support during integration are better. Also, by showing the national EPS as similar to that provided in the e-government website, it will meet customer acceptance and trust; as a result, the adoption of e-commerce will grow.

REFERENCES


Appendix F: Confirmation Letter for identical translation

This is to confirm that Mr. Mohanad Halaweh, PhD researcher asked me to evaluate the transcribed texts provided in his thesis. I performed this activity and can confirm that the Arabic and English versions have identical meaning.

Maher Aljaber
Research Student, Faculty of Technology
De Montfort University, UK
Maheraljaber@yahoo.com

Jehad Al-Amri
Research Student, Faculty of Technology
De Montfort University, UK
Jehad.al-amri@learner.dmu.ac.uk
Appendix G: Description of organisations where data was collected from

-Souq (www.souq.com) is one of the leading auction websites in the Arab world enabling individual sellers and buyers to sell and trade products and services, providing different methods of payment. Souq has more than 10,000 Jordanian active users who buy and sell products over the website. The website has three interfaces for three countries people: Jordan, United Arabic Emirates and Saudi Arabia. (2 participants)

-Royal Jordanian Airlines (www.rj.com) is the National carrier of the Hashemite Kingdom of Jordan. It is the only airline company in Jordan. By the end of 2007, Royal Jordanian has applied an e-Ticketing system which provides its customers with an internet booking engine to book flights online which saves time, money, and effort for the customers. Royal Jordanian was awarded gold for the best website of an Arab carrier in 2007 at the 3rd annual contest held by the Pan Arab Web Awards committee in Dubai. The airline as stated in its website is now collaborating with a leading local web design company to make the website accessible in Arabic, French, Spanish and German, in addition to English in order to enable visitors from all over the world easier access to the website services. (1 participant)

-ESKADENIA Software (www.eskadenia.com) was established in the year 2000 with the objective of being a world-class software vendor in the fields of Telecommunications, Internet, and Enterprise applications. The company has over one hundred and twenty employees, and sales activities in the Middle East, Europe, America and Africa. ESKADENIA Software is specialised in the development of e-commerce applications, web design and portals. ESKADENIA provides e-commerce sites that can be connected to virtually any online credit card payment gateway. (4 participants)

-Specialized Technical Services (STS) (www.sts.com.jo) was established in 1989. It is one of the leading regional providers of business technology solutions. It has provided technology solutions in the banking, government, telecom and education sectors. STS is a leading provider of e-payment solutions and services across the Middle East and North Africa (MENA) region. PayONE™ Gateway, an electronic payment gateway solution, was launched by STS, offers
customers the benefits of making secure online and real-time electronic payments and transfers using multiple payment methods (e.g. credit cards, debit cards and prepaid cards). (1 participant)

-Executive Technologies (www.exetecs.com) is a business technology firm, founded in 2002 to provide consulting and outsourcing services through a network of specialist people in IT services, auditing and security. (1 participant)

-Royal Scientific Society (RSS) (www.rss.gov.jo) is the largest applied research institution and consultation and technical service provider in Jordan, it has 10 technical centres and departments in different fields including an IT centre. This centre is mainly engaged in scientific and technological research and development, consulting and requirements analysis, the development of software for public and private institutions, and the delivery of training services. (1 participant)

-www.Joepay.com is an auction website. It was available in 2007 and is not available now. (1 participant)

-www.azharna.com is online shopping mall delivering gifts such as Flowers, paintings, candles, food items and other Dead Sea products. (1 participant)