ISBN 978-83-60810-14-9
ISSN 1896-7094

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 justifiable, as most existing research conducted in Jordan confirms the security concern in e-commerce and Internet banking, without exploring the issue in depth [14]-[18]. This barrier (i.e. security) makes both Jordanian organizations and individual customers hesitant to participate in e-commerce transactions, and thus reducing the growth of e-commerce. Therefore, security in e-commerce is a vital area of research, 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-

978-83-60810-14-9/08/$25.00 © 2008 IEEE

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 understood 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 experimentations 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 experimentations 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:

> *I think if there is a security company that is recognized internationally, then this shows that they have a list of websites they registered, as well as mentioning they give these websites a reference number, then the customer once entering a certain website can check this reference number or the brand name of this company in the security company's list…not merely a stamp, rather a reference number… this method makes buying over the internet secure.*

> *Well, some websites mention that they have secure payment but this does not mean indeed it is secure unless it is provided by a third party.*

Several participants perceived that if a site is well known then it must be secure, when they were asked how they would check that a certain website was secure or not. Some participants referred to websites that were trusted by others, and relied on the rating scheme that was provided via that website. For example:

> *As I told you the famous company provides security …. I suppose they do that because they respect their customer. Besides, it shows the security policy on the website and details regarding freight and delivery.*

> *I think the issue here depends on the website, I mean if the website is well known and rated by users, then that is secure and includes an actual address and telephone number then this site is secure.....*

> *If I find the payment via PayPal, then I complete the transaction without any reluctance because it is a well known worldwide company. The reputation of feedback on a website and the rating by customers, and their experience with a website gives proof that the website is secure and credible.*

In this last quotation, the participant highlighted the familiarity of an electronic payment service provider such as PayPal, and the influence on security perception that the presence of such a familiar service has. This was also asserted by another participant when he said:

> *I didn't hear any one censure Amazon… you know why - because this website deals with the largest company in the world; like PayPal, it undertakes the security on the website, these websites pay millions for that.*

The reputation of a website was also reported by other participants, and that it is the base upon which customers relied when considering 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.*

> *If I do... I do just from a company I have already dealt with or a company that has a good reputation in Jordan.*

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.

TABLE II.
TANGIBLE AND INTANGIBLE SECURITY FEATURES ON E-COMMERCE WEBSITES FROM CUSTOMERS' PERSPECTIVES

Security features in e-commerce website	**Categorizing of security features**
Padlock	Tangible
Security certificate	Tangible
Transferring between interfaces of the website Website presentation	Tangible
Security policy	Tangible
Acknowledgment via email	Tangible
Third party symbols	Tangible
Physical address , telephone # and email	Tangible
Brief description of the security issues that the customer should be aware of on the website	Tangible
Known identity (company has physical building, i.e. Bank)	Intangible
Support password system	Tangible
Well-known electronic payment gateway such as PayPal	Tangible-Intangible
Famous brand/company	Intangible
International	Intangible
Recognized	Intangible
Trusted	Intangible
Well-known	Intangible
Formal website	Intangible
Respected company, large size	Intangible
Reputable	Intangible
Well-rated	Intangible

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.*

In contrast, however, another participant was optimistic by showing the achievement of her company, and the degree of online acceptance from customers. She commented 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 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, the facilities and services that we provide and our security is not just talk, but the fact that when a customer enters our website and obtains the product that he wants with the same specifications, this happens without any complexity and is easy. This makes them come again because they found our sincerity of treatment. Now we have more than 10,000 active users who buy and sell over our website. Those, once they have tried and succeeded, and have found it is secure, they will then become one of our customers and users of our website....it is just the first experimentation.*

He continued by pointing out that the company website also has a forum where sellers and buyers can chat, get to know each other, share opinions, provide suggestions, report 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* 🔒
>
> *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 responsibility 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 indictors 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 organizations' 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 intangible 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

[1] A. Annie, and A. Earp, "Strategies for developing policies and requirements for secure electronic commerce systems," *1st Workshop on Security and Privacy in E-Commerce at CCS2000*, Athens, Greece, 2000.

[2] S. Hawkins, D. C. Yen, D. C. Chouo, "Awareness and challenges of internet security," *Information Management & Computer Security*, vol. 8, no. 3, pp. 131-143, 2000.

[3] L. Labuschagnce, J.H.P Eloff, "Electronic commerce: the information security challenge," *Information Management & Computer Security*, vol. 8, no. 3, pp. 154-157, 2002.

[4] A. Albuquerque, A. Belchior. "E-Commerce websites: a qualitative evaluation.," *The Eleventh International World Wide Web Conference,* Hawaii**,** 2002.

[5] S. Kesh, S. Ramanujan and S. Nerur, "A framework for analyzing e-commerce security," *Information Management & Computer Security*, vol. 10, no. 4, pp. 149-158, 2002.

[6] S. K. Katsikas, J., Lopez and G. Pernul, "Trust, Privacy and Security in e-business: requirements and solutions," in *Proc. of the 10th Panhellenic Conference on Informatics (PCI'2005)*, Volos, Greece, 2005, pp. 548-558.

[7] F. Bjorck, "Institutional theory: a new perspective for research into IS/IT security in organizations," *Proceedings of the 37th Hawaii International Conference on System Sciences*, 2004.

[8] Z. Shalhoub, "Trust, privacy, and security in electronic business: the case of the GCC countries," *Information Management & Computer Security*, vol. 14, no. 3, pp. 270-283, 2006.

[9] B. Von Solms, "Information security–A multidimensional Discipline," *Computers & Security*, vol. 20, no. 6, pp. 504-508, 2001.

[10] C. Bruce Ho and S. Chang, "Organizational factors to the effectiveness of implementing information security management," *Information Management & Computer Security*, vol. 106, no. 3, pp. 345-36, 2006.

[11] G. Dhillson and J. Backhouse, "Current direction in IS security research: towards socio-organizational perspective," *Information Systems Journa*l, vol. 11, no. 2, pp. 127-153, 2001.

[12] J. Elofe and M. Elofe, "Information security management – a new Paradigm," *Proceedings of SAICSIT*, 2003, pp. 130-136.

[13] W. Salisbury, R. Pearson, A. Pearson and D. Miller, "Perceived security and world wide web purchase intention," *Industrial Management & Data Systems*, vol. 101, no. 4, pp. 165-176, 2001.

[14] N. Al-Qirim "The adoption and diffusion of e-commerce in developing countries: the case of an NGO in Jordan," *Information Technology for Development*, vol.13, no. 2, pp. 107 –131, 2007.

[15] S. Alsmadi,. "Consumer attitudes towards online shopping In Jordan: Opportunities and challenges," *The First Forum for Marketing in Arab countries,* Sharjiha, UAE, 2002.

[16] A. A. Al Sukkar and H. Hasan, "Toward a model for the acceptance of internet banking in developing countries," *Information Technology for Development*, vol. 11, no. 4, pp. 381-398, 2005.

[17] M. Sahawneh, "E-commerce: the Jordanian experience," Royal Scientific Society., 2003.

[18] K. M. Titi, "The impact of adoption electronic commerce in small to medium enterprises Jordanian companies," *International conference in e-business and e-learning,* Amman, Jordan, 2005.

[19] K. Knorr and S. Rohrig, "Security requirements of e-Business processes," Towards the E-Society: E-Commerce, E-Business, and E-Government, *First IFIP Conference on E-Commerce, E-Business, EGovernment,* Zurich, Switzerland, 2001, pp. 73-86.

[20] S. Kesh, S. Ramanujan and S. Nerur, "A framework for analyzing e-commerce security," *Information Management & Computer Security*, vol. 10, no. 4, pp. 149-158, 2002.

[21] A. Sengupta, C. Mazumdar and M. Barik, "e-Commerce security – a life cycle approach," *Saddhana*, vol. 30, no. 2 &3, pp. 119–140, 2005.

[22] A. Zuccato, "Holistic security management framework applied in electronic commerce," *Computer and Security* , vol. 26, pp. 256- 265, 2007.

[23] S. Lichtenstein and P. Swatman, "Effective management and policy in e-Business," *Security e-Everything: e-Commerce, e-Government, e-Household, e-Democracy 14 th Bled Electronic Commerce Conference, Bled*, Slovenia, 2001.

[24] J. Rees, S. Bandyopadhayay, and E. Spafford, "Policy Framework for interpreting risk in eCommerce security," *Communications of the ACM,* vol. 46, no.7, 2003.

[25] A. Sharma and W. Yurcik, "A study of e-Filing tax websites contrasting security techniques versus security perception," *Proceedings of the Tenth Americas Conference on Information Systems*, New York, 2004.

[26] C. Turner, M. Zavod and W. Yurcik, "Factors that Affect the Perception of Security and Privacy of E-Commerce Web Sites," *Intl. Conf. on E-Commerce Research (ICECR),* 2001.

[27] S. Singh, "The social dimensions of the security of internet banking," *Journal of Theoretical and Applied Electronic Commerce Research,,* vol. 1, no. 2, pp. 72 – 78, 2006.

[28] M. Yenisey, A. Ozok, and G. Salvendy, "Perceived security determinants in e-commerce among Turkish university students," *Behaviour & Information Technology*, vol. 24, no. 4, pp. 259-274, 2005.

[29] C. Centeno, "Soft Measures to build security in e-Commerce payments and consumer trust," *Communications & Strategies,* vol. 51, 2003.

[30] S. M. Furnell, "Considering the Security Challenges in Consumer-Oriented eCommerce," *The 5th IEEE International Symposium on Signal Processing and Information Technology,* Athens, Greece, 2005, pp. 534-539.

[31] A. Strauss, and J. Corbin, *Basics of qualitative research: grounded theory procedures and techniques*. SAGE Publication, London, 1990.

[32] S. L. Jarvenpaa, N. Tractinsky, and M. Vitale, "Consumer trust in an -internet store," *Information Technology and Management* , vol. 1, no. (1/2), pp. 45–72, 2000.

[33] B. Suh and I. Han, "The impact of customer trust and perception of security control on the acceptance of electronic commerce," *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 135-161, 2003.

[34] C. M. K Cheung and M.K.O Lee, "An integrative model for consumer trust in internet shopping," *in Proceedings of the European Conference on Information Systems (ECIS)*, Naples, Italy, 2003.

[35] M. Koufaris and W. Hampton-Sosa, "The development of initial trust in an online company by new customers," *Information & Management*, vol. 41, no. 3, pp. 377–397, 2003.

[36] R. Connolly and F. Bannister, "Consumer trust in internet shopping in Ireland: towards the development of amore effective trust measurement instrument," *Journal of Information Technology*, vol. 22, no. 2, pp. 102-118, 2007.

[37] M. Teltzrow, B. Meyer, and H. Lenz, "Multi-channel consumer perceptions," *Journal of Electronic Commerce Research*, vol. 8, no. 1, 2007.