SECURITY IN E-BUSINESS
Understanding Customers Perceptions and Concerns

Ja'far Alqatawna, Jawed Siddiqi
Informatics Research Gruop, Faculity of Art Computing Engineering & Sciences
Sheffield Hallam University, Sheffield, U.K.

Mohammed Hjouj Btoush
Al-Balqa' Applied University, Al-Salt, Jordan

Keywords: e-Business security, Security socio-technical issues, Online customers' security concerns, Security stakeholders, Technological limitations, Qualitative study, Interpretive approach, Jordan.

Abstract: It has become apparent to many security researchers that traditional security approaches are not sufficient to provide adequate security for today's pervasive electronic business environment. We and others argue that security is a socio-technical problem in which its social components are not sufficiently addressed or understood. Our contribution aims to overcome this problem situation, by developing a better understanding of online customers' security perceptions in Jordan. An interpretive approach is employed and general inductive coding process is used to analyse the collected data. On the basis of these study's findings we argue that many customers' related aspects need to be considered in order to elevate e-Business security. These aspects include perceptions and concerns as well knowledge of and interaction with other stakeholders.

1 INTRODUCTION

E-Business security is a multi-faceted problem, and understanding it is not an easy task. It's not enough to address only technical requirements (Confidentiality, Integrity, Availability…etc) in order to increase the security bar. E-Business systems have interconnecting and interacting components (people, software, hardware, procedures and data) and should be looked upon as information systems, with a technological infrastructure and organisational framework, rather than pure technological infrastructure (Katsikas et al., 2005). It is argued in (Alqatawna et al., 2008a; 2008b) the need for multidimensional framework for e-Business security. Such framework should address the needs and the roles of the different stakeholders who may affect or be affected by online security. Our contribution to this framework in this study explores security issues surrounding online customers who are important e-Business stakeholders. Customer represents a direct and interested party who benefits from e-Business in general and from security in particular. Many studies have shown that Internet users in general and e-Commerce customers in particular are concerned about security and privacy over the internet (Paine et al. 2007). In a developing country such as Jordan, companies started to conduct online business activities. Yet, surveys show that customers concerns about security issues are the major obstacles for e-Business diffusion in the country (Alsmadi, 2002; Khasawneh et al., 2009). In contrast to these previous studies, this study provides a deeper insight into the customer perspective of the problem and aims to answer the question of how customers perceive security of the electronic environment and its potential for conducting commercial transitions. How much people are aware about their online security and how they perceive and deal with online risks are important questions to increase our understanding of e-Business security problem. Understanding the customers' social and psychological characteristics could open the door for designing better socio-technical security measures.

Alqatawna J., Siddiqi J. and Hjouj Btoush M.
SECURITY IN E-BUSINESS - Understanding Customers Perceptions and Concerns.
DOI: 10.5220/0002803503190324
In *Proceedings of the 6th International Conference on Web Information Systems and Technology (WEBIST 2010)*, page
ISBN: 978-989-674-025-2

2 STUDY METHOD

Based on the nature of the research question, we have chosen the interpretive qualitative approach as an epistemological and underlying assumption for this study (Myers, 1997). We argue that the exploratory nature of the study requires the use of an approach which provides a deeper understanding of the research situation that generates new ideas that can help to overcome the problems associated with e-Business security. This is best achieved through a knowledge generating approach such as an interpretive one. A purposive sample of Jordanian citizens was recruited as participants in this study. Participants have been chosen because they have had previous experiences with the Internet involving either buying, selling online or just using the internet for online banking, communication and searching for information. The researcher started with convenient sample followed by snowball sample in which the initial participants have been asked to suggest other people who might participate in this study. In total, 27 participants took part in this study. The primary method of data collection was semi-structured interviews. The interviews' purpose was to explore customers' perceptions and expectations regarding information security in the country's e-Business environment. For analysing qualitative data thematic framework analysis was applied (Ritchie et al., 2003).

3 STUDY FINDINGS

There was strong evidence grounded in the data supporting the claim that customers value the notion of e-Business. However, other evidence showed that they have perceptions and serious security concerns which prevented them from performing commercial transactions over the internet. From the analysis carried out five themes involving perceptions and concerns emerged, they are; security and privacy needs; limitation of technical solutions; building trust with supplier; self capability to protect online security and finally threats within the online environment. The five conceptual themes depicting customers' security perceptions are discussed in details below.

3.1 Security and Privacy Needs

Customers' perceived need for security and privacy emerged as a natural requirement that need to be fulfilled to encourage them to use e-Business with confidence. The values of security and privacy were appreciated and requested by most of the study participants who argued that these two aspects are important for them and they will feel safe if these aspects are ensured in e-Business environment. For instance, it was argued that "*security is important and it should exist to protect users from any malicious internet sites*" and regarding privacy, participant believed that "*everybody should have privacy on the internet...it is important requirement*". Privacy needs were expressed in terms such as "*having control over personal information*", "*not being monitored over the internet*" or "*to have your own online space*". Some participants saw no difference between online and offline privacy and believed that privacy should be ensured in both cyber and physical worlds. They argued that accessing or using personal information should be based on the permission of the person who owns this information. Additionally, violation of online privacy was considered unwanted and uncomfortable. In addition, participants emphasised the need to have secure online environment to protect customers. They believed without security it is difficult to use the internet with confidence. Moreover, it was argued that security is important for building trust with the other side of the transaction. Security was understood by them as a mean to "*protect the end users from online threats and to prevent any attempt of malicious act*".

Notably, many participants were able to distinguish between privacy and security as two different constructs. Few used the term privacy to define security or the opposite. This highlights the point that e-Business systems should pay attention to both security and privacy aspects as in some implementation ensuring one can imply compromising the other.

3.2 Limitation of Technical Solutions

Another point revealed in this study was related to the customers' perception about the security of the internet technologies and the ability of the technical security solutions such as personal anti-viruses, firewalls and anti-spywares to provide them with adequate level of security. Many of them believed that internet technologies, which are the backbone for e-Business, have their limitations and not without deficiencies which could lead to many security implications. Based on that, they argued that their level of trust in these technologies is limited. This perception was also fostered by their belief in imperfections of the people developing these applications:

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

Many participants saw that the available security technical controls are unable to completely prevent security threats. They mentioned many cases in which their computers get infected by viruses or hacked despite the fact that they were using all the possible security solutions. This problem was understood by some participants as a result of rapid advancement of internet related technology which is not paralleled with similar advancement in security which gives a window of attack for an attacker to exploit security weakness before they get fixed:

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

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

3.3 Building Trust with the Supplier

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

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

"...Before I use their e-commerce systems I like to read how much security they have and what is going to be if something happed..Also you should check their digital certificate"

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

Although, customers seemed concerned about security, these finding suggested that they appear to be unaware of many security controls and features (third party certificates, encryption, privacy policy…etc) which online merchant usually use to increase customer trust and ensure security. Consequently, they depended on other factors such reputation and recommendation of other to get some kind of online assurance.

3.4 Self-capability to Protect Online Security

When asked about their capability to ensure their online security, participants seemed not confident about this matter and perceived themselves as lacking competence in protecting their security.

They discussed many factors which they believed contributed to this lack of competency. For some of them, there were factors which are out of the online customers' control. In additional to the technical limitation discussed in the previous section, they stressed that the online environment is not controlled and full of unexpected events that could affect their online security. For example, one participant discussed how the popup windows or some links in one website could redirect you to another website that you are not intended to visit, which could be a malicious one. They also thought that whatever they do to ensure security, there are always *"bad guys"* equipped with superior knowledge and skills who can violate their online security:

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

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

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

Also it seemed that many were convinced that only experts could gain the knowledge that can help them to protect their security. Another point emerged from discussing this topic was related to the role of the other stakeholders in relation to customers online security. For instance, it was stated that if the other parties involved in e-Business don't secure their side it will not be enough to secure the customer side. Another aspect of stakeholders that emerged was related to the role of parties such as government and regulatory bodies in helping customers to protect their online security.

3.5 Threats within the Online Environment

When asked about buying or selling over the internet, customers' responses showed that the idea was in principle acceptable, moreover, they were able to identify several potential advantages for e-Business such as saving time, effort and money. However, exploring their actual online behaviours gave the indication that many of them could use internet for many activities expect those involving financial transitions. The study results showed that this reluctance to engage in real e-Business transaction was partially due to customers' fear of being subject to the various security threats associated with the internet environment. Table 1 shows the list of customers' perceived threats of the online environment. Despite the fact that participants believed the internet is useful, most of them were unwilling to provide sensitive information over the internet as they perceived the internet as open and insecure environment which could expose their information to different security risks. The following quote demonstrates this perception:

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

Table 1: List of perceived security threats associated with e-Business.

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

The study also revealed that this perception was not only a general fear of the internet environment, but based on awareness of specific security threats, as shown in Table 1, that customers fear when carrying online commercial transactions. In addition to the common security threats such as *hacking attempts*, *spying* and *virus attacks*, it was also argued that there are possibilities for online impersonation, and deception. One participant argued that *"anybody could create a website and claim that it is representing a company*". Other expressed their fears of transacting with dishonest merchants who might not deliver items, send faulty ones or charge more that the price shown in the website. These perceptions were not always based on the customer personal experience with the merchant, but also on stories of other people who tried to buy product over the internet.

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

4 DICUSSION CONCLUSIONS

Absolute security could be unattainable (Audestad, 2005). Yet many actions can be taken to raise its level in e-Business environment. This research argues for identifying and understanding the different security stakeholders, what they are required to know and what actions need to be taken to increase security in away that provides trustworthy e-Business environment. In such an environment, customers represents a human element that interacts with technological elements which have been designed and secured by technologists who usually don't pay much attention to understand the human element and its social setting (Odlyzko, 2003). In contributing to overcome this problem, this study has aimed to understand the customers' security related issues. On the basis of the study's findings it can be argued that many customers' related aspects need to be considered in order to elevate e-Business security. These security aspects include *perceptions and concerns* as well as *knowledge of and interaction with other stakeholders*

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

At the technical level, the limitations & complexity of the human-made technologies as well as inability of security systems to provide ultimate protection for these technologies are one of the factors that contribute to increase customers' e-Business security concerns. All the recent security reports suggest that vulnerabilities in software are increasing dramatically. For instance, SANS @RISK public vulnerabilities database has reported during 2006-2007 more than 4000 vulnerabilities in Web applications and other commonly used applications such as operating systems, office software and even anti-viruses (SANS, 2009).

Several explanations for this continuous growth of the software security problems have been provided by the security research communities. Security researchers assert that software developers still lack awareness of secure programming techniques and secure software design principles, therefore, vulnerabilities continuo to appear (Ahmad, D., 2007; Howard, M., 2008). Other researchers highlight the negative effect of growing software complexity on security. McGraw (2004) argues that software security represents a critical aspect of the security problem. Moreover, he argues "*internet software applications present the most common security risk encountered today, with software's ever-expanding complexity and extensibility adding further fuel to the fire*". Schneier (2004) describes complexity as "*the worst enemy of security*" because it makes it harder to analysis and test software which increases the chance that software will contain security flows. Thus it seems that all the advances in e-Business applications and their interesting features, offered to online customers, are a result of the increased complexity which in turn affects security.

Our findings show that a specific aspect of customer's knowledge that needs to be considered is awareness of companies' mechanisms to provide online security. Several security protocols and components such as digital certificate and secure socket layer (SSL) have been developed to secure online transactions. In additional to the protection that these mechanisms provide, it is assumed that the existence of these security controls in the company website will positively affect customers' security perceptions and elevate their trust levels (Srinivasan, S., 2004). Unfortunately, when customer is unaware of such controls it is unlikely that they will affect his security perception. In this case he will have limited amount of information to assess security and trustworthiness of online merchant and in case he decide to make online transaction with particular merchant, he might depend on other concerns - appearance, brand name, or just word of mouth - which are not necessarily related to the actual security practices of the merchants.

These findings lead us to conclude that customers concerns about the security of internet applications are legitimate because they still suffer from these technical vulnerabilities which create a barrier to the full engagement in e-Business transactions, this should/must increase the motivation on technology vendors to develop their security skills and practices in order to reduce security holes in e-Business applications.

These findings confirm Turner (2003)'s study which suggests that because customers don't understand technical security controls their perceptions of the website security are formed based on factors such as reputation and recommendation. However, Turner's study didn't highlight the novelty of our findings. These are the need for communicating security to customers and building their awareness of such security controls which arguably could improve their security assessments in two significant ways. First, customers' concerns might be alleviated when they are made aware of these security controls, and furthermore their existence might increase their perception that merchant is secure and trustworthy. Second, we argue that this knowledge empowers customers' to have real controls which can be used alongside with their anecdotal recommendations and common sense perceptions to assess online merchant security.

REFERENCES

Katsikas, S., Lopez, J. and Pernul, G.,2005. Trust, Privacy and Security in E-business, Requirements and Solutions. *Proc. of the 10th Panhellenic Conference on Informatics (PCI'2005)*, Volos, Greece, pp. 548-558.

Alqatawna, J., Siddiqi, J., Akhgar, B., and Hjouj Btoush, M., 2008. Towards Holistic Approaches to Secure e-Business: A Critical Review, *CSREA EEE,* 245-251.

Alqatawna, J., Siddiqi, J., Akhgar, B., and Hjouj Btoush, M., 2008. A Holistic Framework for Secure e-Business, *CSREA EEE,* 257-263.

Paine, C., Reips, U., Stieger, S., Joinson, A., and Buchanan, T., 2007. Internet users' perceptions of privacy concerns and privacy actions. *Int. J. Hum.-Comput. Stud*, 65(6): 526-536.

Khasawneh, A., Al Azzam, I., and Bsoul, M., 2009. A study on e-commerce security in Jordan. *International journal of electronic finance,* 3 (2), 166-176.

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

Myers, M., 1997. Qualitative Research in Information Systems, *MIS Quarterly* 21(2).

Ritchie, J., Spencer, L., and O'Connor, W., 2003. Carrying out qualitative analysis. In : Qualitative research practice. Edited by Ritchie, J., & Lewis, J., *SAGE*, London.

Audestad, J. A. 2005. Four reasons why 100% security cannot be achieved, *Telektronikk,* vol. 101, pp. 38.

Odlyzko, A., 2003. Economics, psychology, and sociology of security. *Lecture Notes in Computer Science,* pp. 182-189.

Suh, B., and Han, I., 2003. The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce,* vol. 7, pp. 135-161.

Flavián C., and Guinalıú, M., 2006. Consumer trust, perceived security and privacy policy. *Industrial Management and Data Systems,* vol. 106, pp. 601-620.

Salisbury, W. D., Pearson, R. A., Pearson A. W. and Miller, D. W., 2001. Perceived security and World Wide Web purchase intention. *Industrial Management and Data Systems,* vol. 101, pp. 165-176.

Lee, P. M., 2002. Behavioral model of online purchasers in e-commerce environment. *Electronic Commerce Research,* vol. 2, pp. 75-85.

SANS Institute, "SANS Top 20 vulnerabilities," [Online] http://www.sans.org/top20, accessed 26/8/2009.

Ahmad, D., 2007. The contemporary software security landscape. *IEEE Security & Privacy,* vol. 5, pp. 75-77.

Howard, M., 2008. Becoming a Security Expert. *Security & Privacy, IEEE,* vol. 6; 6, pp. 71-73, 2008.

McGraw, G., 2004. Software security. *Security & Privacy, IEEE,* vol. 2; 2, pp. 80-83.

Schneier, B., 2004. *Secrets and Lies: Digital Security in a Networked World.* Wiley New York.

Srinivasan, S., 2004. Role of trust in e-business success. *Information Management and Computer Security,* vol. 12, pp. 66-72.

Turner, C., 2000. How do consumers form their judgments of the security of e-commerce web sites, *ACM/CHI2003 Workshop on Human-Computer Interaction and Security Systems.*