Available online at www.sciencedirect.com
SciVerse ScienceDirect
Procedia - Social and Behavioral Sciences 62 (2012) 1265 – 1270
Procedia Social and Behavioral Sciences

WC-BEM 2012

Consumers' issues and concerns of perceived risk of information security in online framework. The marketing strategies

Theodosios Tsiakis*

Department of Marketing, Alexandrian Technological Educational Institute of Thessaloniki, P.O BOX 141, Thessaloniki 57400, Greece

Abstract

Internet (web) transactions are subject to numerous information security threats. Consumers' trust is fundamental in web transactions and is influenced by perceived information security. The primary factor/reason causing consumers lack on e-business is perceived security risks associated with online transactions. There is a certain relationship between electronic security concerns and customer online shopping attitudes and behavior. Customer security in e-business environment is an on going research issue especially in current electronic marketing field. A marketing strategy can strengthen of reduce the security of an information security company The purpose of this paper is to try to identify, illustrate and analyze the current and future directions in consumer issues and concerns of perceived risk of information security. Also to illustrate the current status of security issues and concerns for online buying shopping attitudes and behavior.

Keywords: Information Security, perceived risk, trust, e-business;

1. Introduction

Current rapid technological achievements and developments that are observed especially in the last decade have substantially made Internet market to be used by everyone. A plethora of products' and services' purchases are now operated online through websites and internet applications, contributing to the extent of e-business a one of the most essential commercial tool. But that does entail that all consumers are participating in online transactions as part of the Internet boom. Online shopping is the process where consumers purchase products or services simply by using the Internet. The act of shopping through the Internet raises questions about consumers/customer prothesis to shop online. Although the Internet has great potential for consumer value, there seems to be a discrepancy between the number of consumers who visit a website and the number of actual purchases being made (Ab Hamid, 2008) (Chuleeporn & Corpus, 2006). Furthermore, e-business and in parallel intention to shop online is still problematic due to lack of trust and perceived security risk of on line transactions. Because buyers are capable to have physical, tangible proof of the goods in advance, they always perceive a greater risk than shopping brick-and-mortar (Sheng & Liu, 2009). The issue then is how to effectively and efficiently induce a sufficient level of initial online trust so that successful transactions can be fulfilled and the e-market to stay competitive (Wu et al., 2010). Thus, marketers effort need to be concentrated to the design of web sites in such a way that they can communicate with their consumers effectively, efficiently and it most of all secure (Mann & Sahni, 2011). Websites according to (Flanagin

* Corresponding Author name. Tel.: +302310791652
E-mail address: tsiakis@mkt.theithe.gr

 doi:10.1016/j.sbspro.2012.09.216

& Metzger, 2007) can "be conceptualized as information repositories that represent organizational or individual sources, while also reflecting the characteristics of those sources through design features of the sites themselves". Websites must relate to characteristics as confidentiality, integrity, availability (CIA model) of information, non-repudiation of communication and protection of personal privacy.

2. Overview of current state

In the classic, traditional shopping context, consumers were passive recipients of marketing information (Schrank & Dubinsky, 2004). With the utilisation of advanced Information and Communication Technologies (ICT) consumers are now active users, co-producers of information and firms are collecting more customer information than ever before (Malhotra & Malhotra, 2011). As Internet usage is increasing and online shopping accordingly, marketers need to study and understand how the transformation in the online retailing environment relates to dissatisfaction and distrust especially in those countries whose marketing infrastructures are well developed (Limbu et al., 2011) (Chuleeporn & Corpus, 2006). Online marketing transactions necessitate online customer trust in order for customers to place an order online and even submit his or her financial information and other personal data in undertaking other financial transactions (Yazdanifard et al., 2011). Consumers should have an understanding of online security and privacy risks.

Consumers always perceive a certain degree of risk when they are engaged in buying situation. Risk that a consumer will experience according to (Jahankhani, 2009) is a function of two variables: the amount at stake (consequences) and the individuals feeling of subjective certainty of success or failure. (Chang, 2010) mention that the degree of risk is based on two variables, "consumer purchasing decisions regarding the desired results" and "degree of uncertainty".

In the electronic environment we are concerned with subjective (perceived) risk and not "real world" (objective) risk (Vincent-Wayne, 1999). Consumers perceived risk increases with uncertainty and magnify by the associated negative consequences. In order for consumers to decrease perceived risks, they use several strategies, such as brand loyalty, store image or word-of-mouth, either to confirm their buying decision or reduce the uncertainty they feel about the decision (Schrank & Dubinsky, 2004). Perceived risk can prevent customers from purchasing from an online retailer (Yazdanifard, 2011). Perceived risk is defined as "assessment of uncertainties or lack of knowledge about the distribution of potential outcomes and the uncontrollability of outcome attainment" (Ab Hamid, 2008). Bauer (1967) were the first to introduce the concept of perceived risk to the marketing literature and represented consumer purchase action as a risk-taking behavior.

Online trust is "the extent to which a person perceives the credibility and benevolence of the other party with which he or she first interacts in an online environment" (Wu et al., 2010). Trust is considered to have a positive influence on customers' perceptions and leads to consumer engagement in internet shopping (Yazdanifard, 2011). Initiating, building, and maintaining trust between buyers and sellers is a key facilitator for successful e-business regarding trust definitions perspectives (i. context characteristics, ii. trustor properties and iii. characteristics of the trusted object) (Grabner-Krauter et al., 2006). (Zhou, 2011) identified four factors that affect online initial trust. The first is associated with website characteristics (information quality and website quality). The second concerns consumer characteristics (trust propensity and moderation effect on initial trust. The third category is connected with online vendors (reputation as a trust signal, company size, willingness to customize and brand image). The last is associated with third parties (trust seals, brand association and structural assurances). Trust of an online service is not merely based on objective assessments, but that it can arise from up to five different sources: users' inherent personality, knowledge based on users' prior experiences, institutional assurances from providers, calculative assurances from providers, and cognitive assurances from third parties (Soumya et al., 2011). The above five sources reflect both the predispositions of users and the assurances of providers. Literature shows that researchers have different views about how trust and perceived risk are related. Figure 1 summarizes the four types of relations identified by researchers (Lim, 2003).

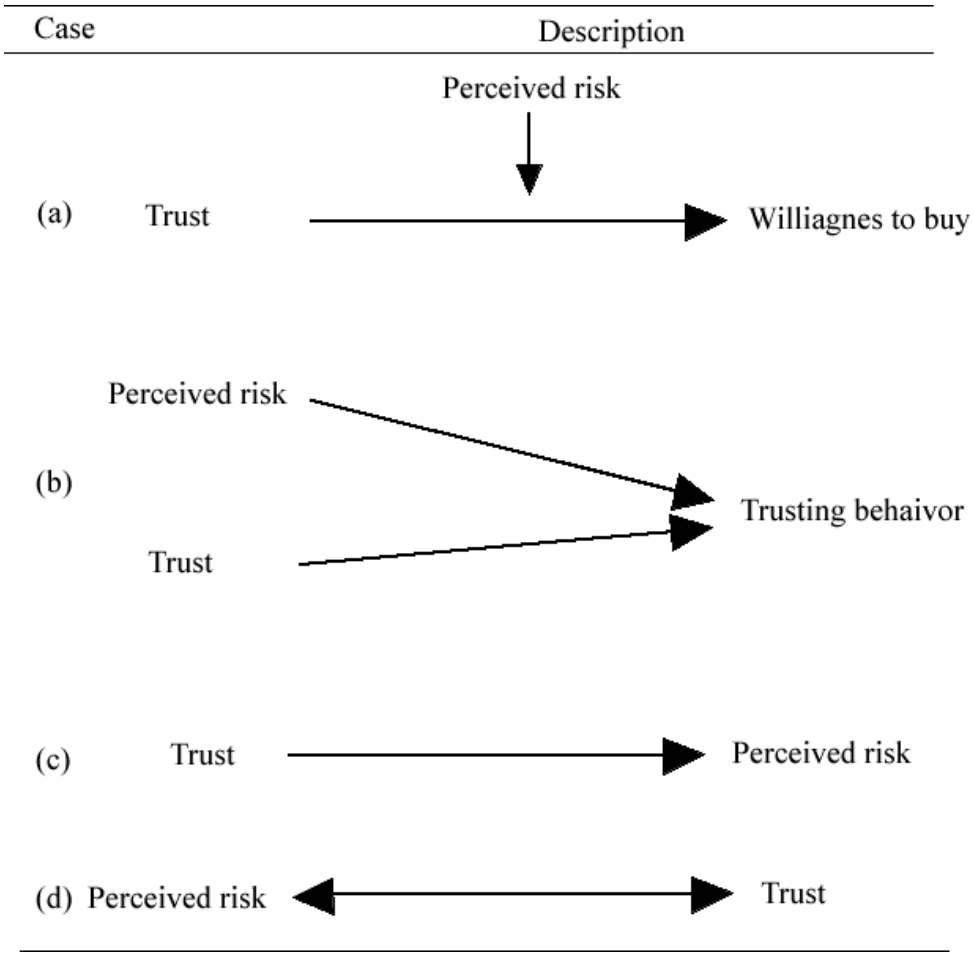

Figure 1. Four types of relations between trust and perceived risk, adopted from Lim, (2003).

3. Current research

Risk is the "combination of the probability of an event and its consequence when there is at least the possibility of negative consequences" (Asnar & Giorgini, 2008). Perceived risk simply is the uncertainty that consumer confront when he is not capable to prognosticate the consequences of his purchase decisions general. Perceived risk arise when consumer is uncertain about the advancement of his shopping action. (Lim, 2003) in a marketing context defines perceived risk as ''the nature and amount of risk perceived by a consumer in contemplating a particular purchase action''.

The dimensions of perceived risk were defined by a number of researchers (Schrank & Dubinsky, 2004) (Jahankhani, 2009) (Ming-Chi, 2009). The paper array the following six (Table 1):

Table 1. Types of Perceived risk

Types of Perceived risk	Definition
Performance risk	is the probability that the product will malfunction and not operate as it was designed and advertised
Social risk	describes the fear that a product or service will lead to a loss of status in one's social group
Financial risk	refers to the probability that a purchase will result in monetary loss.
Psychological risk	the possibility that use of a product will result in inconsistency with consumer's self-image.
Time risk	the probability that a purchase results in loss of time when making a bad purchasing decision by wasting time researching and making the purchase
Physical risk	the probability that a purchased product or service will pose in a threat to human health and safety

The total amount of perceived risk may be a constant while the levels of the types of perceived risk vary with the elements of the situation (Predmore et al., 2007) (Equation 1):

$$\text{Total Perceived Risk} = \Sigma \text{ risk} = \text{evaluation of functional} + \text{physical} + \text{financial} + \text{social} + \text{psychological} + \text{time}$$

Technology Acceptance Model (TAM) is a theoretically justified model, based on the theory of reasoned action (TRA), is intended to examine and explain information technology adoption proposes that attitude towards using a system is influenced by two critical determinants of users' belief: one is perceived usefulness and the other is perceived ease of use. TAM manifest that the use (actual behavior) of IT is determined by individual's intention to use the technology and that one's intention is determined by the person's attitude, as well as perceived usefulness and ease of use and relates to intention and finally to behavior (an increase in perceived usefulness leads to a greater intention to use). Perceived usefulness (PU), is defined as the extent to which a user subjectively believe that the use of a new technology or a system will be useful or will improve his/her performance. Perceived ease of use (PEOU), is defined as the degree to which an individual believes that using a technology or a system will be effortless. (Ab Hamid, 2008) (Huang et al., 2011) (Ming-Chi, 2009) (Chung-Chi & Jyh-Shen, 2010).

4. Discussion

Tian et al., (2010) indicate that the majority of literature about security in e-commerce is mainly focused on security implementation, security effectiveness and few only study consumers' perceived security risks in e-commerce. Security in an online retailing context, refers to consumers' perceptions about the security both of the online transactions as well as the protection of financial information that accompany the transaction from unauthorized access and further is categorized into financial security (concern about providing financial information) and non-financial security (relating to revealing personal information) (Limbu et al., 2011).

People's perception of information security is determined by several perceivable factors, such as the perceived Knowledge, Controllability, Awareness, Severity and Possibility, which is different from the real security level of an information system (Huang et al., 2011). Consumers are reluctance to complete a simple online purchase primarily due to risk concerns and this sets perceived risk as a prominent barrier (Ming-Chi, 2009). From the perspective of consumers, security control is a quality of services that ensures "freedom from danger, risk, or doubt" (Soumya et al., 2011). Threats to assets are interruption, interception, modification and fabrication (in retailing or service firms, interruption is most significant) (Yeh & Jung-Ting Chang, 2007). Information security countermeasures involve various methods (e.g. physical, procedural, hardware, software, and personnel methods) that are employed to detect, prevent or minimize losses associated with the threats to an information system (Zhang et al., 2009). The virtuality and consequently the lack of control, cause great uncertainty and risk to e-(and m-)commerce and the sequent security problems will increase users' perceived risk and decrease the usage intention of electronic payment (Zhou, 2011). Security, which involves a complex interaction between technical, organizational and behavioral factors like

cryptography, digital signatures etc that aim at protecting users from the risk of fraud, hacking or "phishing", and has a positive influence on the intention to purchase online (Roca et al., 2009) (Amitava & Rahul, 2008). Security is protection against such threats and is mainly concentrated in a technical ways while trust and risk are related more adjustable to human concepts. Information security in business context is defined by (Ab Hamid, 2008) "as the subjective probability with which consumers believe that their personal information will not be viewed, stored or manipulated during transit or storage by inappropriate parties, in a manner consistent with their expectations".

References

Ab Hamid, N. (2008). Consumers' behaviour towards Internet technology and Internet marketing tools. *International Journal of Communication*, 3(2), 195-204.

Amitava, D, and Rahul, R. (2008). Dynamics of organizational information security, *System Dynamics Review 24*(3), 349–375.

Asnar, Y. and Giorgini, P. (2008). Analyzing Business Continuity through a Multi-Layers Model. In *Proceedings of the 6th International Conference on Business Process Management (BPM 2008)*, Milan, Italy.

Bauer, R. (1967). Consumer behavior as risk taking. In: Cox, D. (ed.), Risk Taking and Information Handling in Consumer Behavior, Harvard University Press

Chang, A.J.T. (2010). Roles of Perceived Risk and Usefulness in Information System Security Adoption, In Proceedings of 2010 IEEE International Conference on Management of Innovation and Technology (ICMIT).

Chuleeporn, C., and Corpus C. (2006). Consumer perception of online shopping. Issues in Information Systems, 7(2), 177-181.

Chung-Chi, S. and Jyh-Shen C. (2010). The impact of perceived ease of use on Internet service adoption: The moderating effects of temporal distance and perceived risk. *Computers in Human Behavior 26,* 42–50.

Flanagin, A. and Metzger, M. (2007). The role of site features, user attributes, and information verification behaviors on the perceived credibility of web-based information, *New Media Society* 9, 3-19

Grabner-Krauter, S., Kaluscha, E. and Fladnitzer. M. (2006). Perspectives of online trust and similar constructs: a conceptual clarification. In *P*roceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet (ICEC '06). ACM, New York, NY, USA, 235-243.

Huang, D., Rau, P., Salvendy, G., Gao, F. and Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies, 69*(12), 870–883.

Jahankhani, H. (2009) The Behaviour and Perceptions Of On-line Consumers: Risk, Risk Perception And Trust. International Journal of Information Science and Technology', International Journal of Information Science and Management, 7 (1) 79-90

Lim, N. (2003). Consumers' perceived risk: sources versus consequences, *Electronic Commerce Research and Applications 2*, 216–228.

Limbu, Y., Wolf, M. and Lunsford, D., (2011). Consumers' perceptions of online ethics and its effects on satisfaction and loyalty, *Journal of Research in Interactive Marketing, 5*(1), 71-78.

Malhotra, A. and Malhotra, C. (2011). Evaluating Customer Information Breaches as Service Failures: An Event Study Approach. *Journal of Service Research, 14*(1), 44-59.

Mann, B. and Sahni, S. (2011). Inter-Relationship of Web Site Interactivity and Customer Outcomes: Building Trust in Internet Banking Web Site, *Global Business Review, 12*(1), 99–115.

Ming-Chi, L. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications 8*(3), 130-141.

Predmore, C., Rovenpor, Manduley, A., Radin, T. (2007). Shopping in an age of terrorism: Consumers weigh the risks associated with online versus in-store purchases. *Competitiveness Review: An International Business Journal incorporating Journal of Global Competitiveness, 17*(3), 170-180.

Roca, J., Garcıa, J. and de la Vega J. (2009). The importance of perceived trust, security and privacy in online trading systems, *Information Management & Computer Security, 17*(2), 96-113.

Schrank, H. and Dubinsky, A. J. (2004). Effect of brand name on consumers' risk perceptions of online shopping. *Journal of Consumer Behaviour 4*(1), 40–50

Sheng, M. and Liu, T. (2009). Reducing Consumers' Perceived Risk through Website Service Quality Cues in C2C E-Commerce Trading, In *P*roceedings of the International Conference on Management and Service Science, 2009. MASS '09.

Soumya R., Terence O., Sung K., (2011). Security Assurance: How Online Service Providers Can Influence Security Control Perceptions and Gain Trust. *Decision Sciences, 42*(2) 391–412.

Tian, Z. Xu, H., and Xu, N. (2010). Consumers' Perceived Security Risks in E-commerce: A Survey Study, In *P*roceedings of the 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 532–535.

Vincent-Wayne, M. (1999). Consumer perceived risk: conceptualisations and models, *European Journal of Marketing, 33*(1/2), 163-195.

Wu, G., Hu, X. and Wu, Y. (2010). Effects of Perceived Interactivity, Perceived Web Assurance and Disposition to Trust on Initial Online Trust. *Journal of Computer-Mediated Communication, 16,* 1–26.

Yazdanifard, R., Hoe F., Islam, M. and Emami, S. (2011). Customer's Information Security Management System in E-commerce, In *P*roceedings of the 2011 International Conference on Software and Computer Applications IPCSIT vol.9, 187-191.

Yeh, Q. and Jung-Ting Chang, A. (2007). Threats and countermeasures for information system security: A cross-industry study, *Information & Management 44*, 480–491.

Zhang, J., Reithel, B. and Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17*(4), 330-340.

Zhou, T. (2011). The effect of initial trust on user adoption of mobile payment. *Information Development, 27*(4), 290–300