2009

CUSTOMERS' PERCEIVED SECURITY: RELATIVE EFFECTIVENESS OF TRUST TRANSFERENCE MECHANISMS

Anupam Kumar Nath
University of North Carolina at Greensboro, aknath@ungcg.edu

Ruth C. King
University of North Carolina at Greensboro, rcking@uncg.edu

CUSTOMERS' PERCEIVED SECURITY: RELATIVE EFFECTIVENESS OF TRUST TRANSFERENCE MECHANISMS

Anupam Kumar Nath
University of North Carolina at Greensboro
aknath@uncg.edu

Ruth C King
University of North Carolina at Greensboro
rcking@uncg.edu

ABSTRACT

Security concerns pose a bigger threat for less known web vendors because of their lack of reputation. However, trust transference provides a mechanism for web vendors to get a higher level of trust. We utilized an experimental design to examine the effect of two trust transference mechanisms on the perceived security of customers for a less known organization. Results of our study indicate that a less known organization can improve its perceived security for its customers through the use of trust transference mechanisms. Our results have implications for developing competitive positioning strategies for less known web vendors.

Key Words
Online Security, Perceived Security, Trust Transference Mechanism

INTRODUCTION

The U.S. Census Bureau forecasted that online retail sales in the USA will grow from $172.4 billion to $328.6 billion from 2005 to 2010 (Source needed). However, in 2006 alone, $2 billion or about 2% of online spending was lost due to consumers' concerns about security of electronic commerce (InternetRetailer.com, 2006). Web retailers employ multiple security mechanisms to protect against security threats. However, most of these precautions are highly technical and not transparent to e-commerce consumers who may not understand the technical nuances of these security features. Moreover, in situations that involve risk, the objective, scientific perspective is usually different from the subjective, intuitively grounded one (Powell et al., 1997). To provide assurance and develop consumer trust in e-commerce, it is important that companies not only incorporate the technology necessary to protect data and consumer information but provide a mechanism by which customers will feel secure during participation. This aspect, known as perceived security, is defined as "the level of security that users feel when they are shopping on e-commerce sites" (Yenisey et al., 2005). Extant research (Furnell and Karweni, 1999; Chou et al, 1999; Dong-Her et al, 2004) identifies the lack of perceived security for online consumers as a primary obstacle to e-commerce growth. It is important for ecommerce companies to deploy technical measures for securing transactions as well as to take steps that will increase customers' perceived security on their web sites.

Reputation is associated with the organization's credibility and it is result of the comparison between what the company promises and what they eventually fulfill. However, reputation needs to be earned overtime through repeated interaction with the consumers (Casalo et al.2007). Perceived reputation has a strong impact on customers' overall perception of a web vendor (Jarvenpaa and Tractinsky, 1999). However, lack of reputation creates a major obstacle for the less known entrant companies' business. Security concerns pose a bigger threat for less known companies because of their lack of reputation. Therefore, it becomes very difficult for new or relatively unknown organizations to have a good reputation in the beginning that can help them to gain higher perceived security of their customers.

A good reputation is hard to attain in a short period of time. However, trust transference provides a mechanism for companies to get a higher level of trust (Stewart, 1999, 2003). Using trust transference, the involvement of a trusted third party may increase a customer's trust in the transaction as well as in the less know web vendor. The trust transferred from a reputed third party provides assurances that help to increase trust in the less known organizations, particularly when there is no history or firsthand knowledge of the less known web vendor (McKnight et al., 1998). The inclusion of a trusted third party in a transaction can positively influence customers' perceived security of the

lesser known web vendor. Hence, we examine if a less known web vendor can achieve higher perceived security by associating itself with a trustworthy entity with a high reputation and our research is guided by the following research question

How do the trust transference mechanisms affect customers' perceived security towards a less known web vendor?

Specifically, we utilize an experimental design to examine the effect of two trust transference mechanisms on the perceived security of customers for a less known organization. In addition, we compare the relative effectiveness of two trust transference mechanisms, including third-party checkout and electronic marketplace participation, in increasing customers' perceived security towards a less known web vendor. Results of our study indicate that a less known organization can improve its perceived security for its customers through the use of trust transference mechanisms. Our results have implications for developing competitive positioning strategies for less known organizations and for resource allocation for investments in technical security and the development of inter-organizational alliances to improve perceived security for online consumers.

LITERATURE REVIEW, THEORY AND HYPOTHESES DEVELOPMENT

Online privacy and security have always been major obstacles for e-commerce success (Cranor et. al.,1999, Ahuja et. al.,2003, Kim et. al.,2004). In many studies, security and privacy concerns have been considered as a single construct because of their huge overlapping as concepts in the e-commerce world (Belenger et al., 2002). While much e-commerce research considers privacy and security as a single construct, they are very distinct concepts (Flavián and Guinalíu , 2006, Belenger et al., 2002) . Privacy issues in the online environment include 'spam', usage tracking and data collection, choice, and the sharing of information with third parties (Wang et al., 1998). On the other hand, a security threat is a "circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse" (Kalakota and Whinston, 1996). Security, then, is the protection against these threats (Belanger et. al., 2002). The lack of appropriate security controls in electronic commerce can lead to privacy issues. The focus of our study is the impact of trust transference mechanisms on perceived security. A summary of some of the important studies on perceived security are presented in table 1.

Study	***Independent Variables***	***Position of the Perceived security construct in the research model***	***Findings***
Chellappa and Pavlou,2002	Encryption, Protection, Verification, Authentication	Dependent variable and a antecedent of Trust in EC transaction	Encryption, Protection, Authentication have significant increase on perceived security
Suh and Han,2003	Strength of Security control	Dependent variable as well as an antecedent of e-commerce acceptance	Perceived Strength of Security control increases e-commerce acceptance
Yenisey et al., 2005	Security features indicators	Dependent variable	Security feature indicators positively influence intention to buy
Kim et. al.,2007	Awareness as moderating variable of perceived security	Dependent variable	Awareness of security measures has a strong positive effect on the importance of the security measures

Table1: Summary of the existing study on Perceived Security

Chellapppa and Pavlou(2002) found that customers' perceived security can be increased through the appropriate use of technical security features like encryption, protection and authentication. Suh and Han (2003) argued and empirically tested that perceived security can be increased by providing the customers' a sense of control over security. Yenisey et al.(2005) found that customers' buying intention can be positively influenced by having security features indicators in place. Kim et al., (2007) empirically verified that customers' perceived security can be positively influenced by creating awareness of the security measures taken by an ecommerce vendor. While all these studies have considered perceived security as their variable of interest, they do not consider that the security features on an organization's web site may play different roles based on the nature of the organization. For example, a new and relatively less known organization may not be able to develop the level of perceived security from the same

technical security controls as an organization with an established reputation. Existing studies on perceived security do not take into account trust transference mechanism as a way to increase customers' perceived security.

While purchasing using web, a customer usually does not come into contact with any physical entity or representative of the web vendor. Therefore, the role of the perceived reputation of the organization takes increased importance. This is particularly true for relatively less known organizations that do not have the relational history to establish a reputation in the marketplace. Reputation provides assurances of the other party's ability, integrity, and goodwill, which in turn help to increase trust, particularly when the parties have not interacted before and hence do not have firsthand knowledge of each other (McKnight et al., 1998). Reputation is a valued asset and sellers usually try to avoid getting a bad reputation (Chiles & McMackin, 1996). Perceived Reputation is the extent to which buyers believe that the selling organization is honest and concerned about its customers (Doney & Cannon, 1997). The existing literature suggests that the perceived reputation of a company plays an important role in forming the customer's overall perception of the company (Jarvenpaa and Tractinsky, 1999). Since perceived security is a factor in the overall perception of the company (Jarvenpaa and Tractinsky, 1999), it is reasonable to infer that the perceived reputation of the company will affect customers' perceived security. A good reputation signals forbearance from any opportunism in the past. Hence, reputation requires a long-term investment of resources, effort, and attention to customer relationships (Smith & Barclay, 1997); it is a challenge for a relatively new less known organization to establish reputation in a short period of time.

However, a relatively new or less known company can gain trust through trust transference by associating themselves with a trusted party The concept of Transference based trust is based on the cognitive balance theory (Heider 1958). Balance theory (Heider 1958) is focused on the valence of relations between actors (Stewart,1999). Trust transference theory suggests that when confronted with a new target, an individual bases trust in the new target on trust in associated targets in a way that re-establishes balance. If a person has dissimilar level of relationships with associated parties then the individual experiences dissonance. People tend to reduce such dissonance (Festinger 1954). Given two positive relations, where Alice trusts Bob and Bob is associated with Carol, balance theory predicts that the third relation will also be positive and Alice will trust Carol. Trust transference theory suggests that a transfer of trust occurs in forming this third relationship (Stewart, 1999; 2003).

Following trust-transference theory, we posit that when a customer is conducting an online transaction, the involvement of a trusted third party will increase the trust in the online transaction as well as the web vendor. In other words, if a transaction is facilitated or supported by a trusted third party, then the facilitation will positively influence the relationships between customers" perception of the web vendor and the perceived security. Trust may be transferred from different kinds of sources (Stewart, 1999). In the context of WWW we have considered two mechanisms for trust transference- third party checkout and marketplace participation.

Milliman and Fugate (1988) argued that trust transfer can occur from a place or an industry association to an entity. They found that a salesman could transfer the burden of establishing trust from himself to a "proof source"—specifically that the salesman could co-opt a prospect's trust in an industry association. Milliman and Fugate (1988) explained that the proof source offered verifiable evidence of the salesperson's claims and therefore led to a greater intention to buy on the part of the client. Similarly in e-commerce, association with a well reputed and trusted third party can help a relatively unknown (or less reputed) e-commerce vendor to gain their customers' trust (Stewart, 2003). Previous work on trust transference also suggests that transfer may work through different processes(e.g. Stewart,2003).It may occur based on a communication process in which either the target or a trusted third party exerts direct influence on the trustor. In addition, trust transference may be based on a cognitive process where the mere knowledge of the relationship between the target and another source of trust induces the transfer of trust to the target.

A trusted Third Party checkout mechanism is one such mechanism where a trusted third party wields direct influence on the trustor. Third party Checkout is an online payment processing service provided by a third party such as Paypal or Google to simplify the process of paying for online purchases. Involvement of a trusted third party to facilitate transaction with a less known web vendor can serve as the source of trust transference for a customer. The transference based trust gained by a less known company from a trusted third party checkout system can help the less known company to gain higher level of perceived security. However, if a web vendor has highly visible security features in place on their website then that company might have a higher level of perceived security then a web vendor with less visible security features. Hence, the level of trust transference and perceived security

might not be same for a web vendor with highly visible security features and a web vendor with less visible security features. Nevertheless, since a trust transference mechanism (i.e. Third party checkout) is in place, based on Trust Transference theory we can infer that perceived security of both web vendors will increase.

Hence, we propose the following hypotheses to test the increased levels of perceived security through the transference of trust from association with a third party checkout System.

H1a: A Less known company with highly visible security measures will have less perceived security than a less known company with highly visible security measures and Third party checkout .(i.e. $\boldsymbol{PS_{(LKHS)} < PS_{(LKHSG)}}$*)*

H1b: A Less known company with less visible security measures will have less perceived security than a less known company with less visible security measures and Third party checkout .(i.e. $\boldsymbol{PS_{(LKLS)} < PS_{(LKLSG)}}$*)*

Another source that can provide transference based trust to a less known company is an electronic marketplace. Electronic marketplaces (EMP) are independently owned, IT-enabled intermediaries that connect many buying organizations with many selling organizations (Soh et. al., 1998). Success stories of marketplaces like Amazon and eBay have proved the importance of marketplaces in e-commerce. In general a marketplace has to play three important roles: matching buyers and sellers, facilitation of transaction, providing Institutional Infrastructure for transactions (Bakos, 1998). Marketplace participation is another such mechanism where trusted third party wields direct influence on the trustor. Even though a web vendor has less or no reputation in the existing market, transference based trust gained by the less known company through marketplace participation can help that company gain higher level of perceived security. A web vendor that participates on a marketplace might have highly visible security features or less visible security features. However, considering the presence of trust transference mechanism (i.e. trusted marketplace), we can deduce that for both the web vendors perceived security will increase.

Thus, we propose the following hypotheses

H2a: A Less known company with highly visible security measures will have less perceived security than a less known company with highly visible security measures and marketplace participation. (i.e. $\boldsymbol{PS_{(LKHS)} < PS_{(LKHSM)}}$*)*

H2b: A Less known company with less visible security measures will have less perceived security than a less known company with less visible security measures and marketplace participation.(i.e. $\boldsymbol{PS_{(LKLS)} < PS_{(LKLSM)}}$*)*

The following section provides details on our research method to test these hypotheses.

RESEARCH METHOD

We used an experiment to find out the group difference between perceived security of less known web vendors that participate in third party checkout mechanism or in electronic marketplaces. The perceived security of the web vendors themselves serve as the control group in our experiment.

Experiment Design

A challenging aspect of our experiment design was to categorize the vendor's website in terms of the security measures visible on their website. We have used the approach in Belanger et al. (2002). Based on the existing literature and the content analysis of more than 100 web vendors' site, we have identified the methods/techniques taken by vendors to increase the potential customers' perceived security. While there may be security mechanisms running in the background, for the purpose of our study we were only interested in the security mechanisms which are visible to the customers on the web vendor's site. These mechanisms include:

(a) Presence of Third party security seal (Belenger et al., 2002, Kim et. al, 2004)
(b) Presence and clarity of Security statement (Yenisey et al., 2005),
(c) The website's emphasis on login name and strong password request (Yenisey et al., 2005)
(d) The website's emphasis on security in file transfers over the internet (Chellappa and Pavlou,2002, Yenisey et al., 2005)
(e) Visibility of the website's encryption strategy
(f) The website's distribution of security items within its body (Yenisey et al., 2005).

Based on these criteria, a group of experts were asked to categorize the web sites as "Highly Visible Security Features "or "Less Visible Security Features". The selected web vendors were pre tested with 30 participants as well as with colleagues to make sure that the web vendors have been classified properly. In our experimental setup we have included cells for a less known web vendor with highly visible security features and for less known web vendor with less visible security features. As control group, we have included one cell for a less known web vendor with highly visible security features and a less known web vendor with less visible security features. Both of these web vendors are doing business without any third party involvement.

To examine the effect of third party checkout on perceived security, we have selected two other web vendors for the first two cells of the treatment group. In one cell we have assigned a less known web vendor with highly visible security features and with Google checkout as an alternative transaction method. In the other cell, we have assigned a less known web vendor with less visible security features and with Google checkout as an alternative transaction method.

We have included two other cells as treatment groups to identify the effect of marketplace participation on perceived security. In one cell we have assigned a less known web vendor with highly visible security features that facilitates its own transaction processing system and participates on the marketplace. In the other cell we have assigned a less known web vendor with less visible security features that maintains its own transaction processing system and also participates on the marketplace.

In our experimental setup, to control for the effect of price, we have made sure that the company participating on a marketplace is offering the same price on their own website as well as on the marketplace site for the product the participants were asked to buy. We have also made sure that the web vendor is offering the lowest price for that product on the marketplace. To have more control over the experiment we have made sure that all the selected websites have similar sort of products to offer. In our experimental setup all the web vendors offer (not limited to) electronic products like mp3 player, ipod, digital picture frame. An overview of all the six cells of the design and notations used in rest of the paper has been presented in the figure1.

Less Known Highly Visible Security Measure Web Vendor: As Is	
With Third Party Checkout	Marketplace Participation
Less Known Less Visible Security Measure Web Vendor: As Is	
With Third Party Checkout	Marketplace Participation

Figure1: Experimental setup

$PS_{(LKLS)}$	Perceived Security of the customers towards Less Known Less Secured Company
$PS_{(LKHS)}$	Perceived Security of the customers towards Less Known Highly Secured Company
$PS_{(LKLSG)}$	Perceived Security of the customers towards Less Known Less Secured Company with Google checkout
$PS_{(LKHSG)}$	Perceived Security of the customers towards Less Known Highly Secured Company with Google checkout
$PS_{(LKLSM)}$	Perceived Security of the customers towards Less Known Less Secured Company with Marketplace participation
$PS_{(LKHSM)}$	Perceived Security of the customers towards Less Known Highly Secured Company with Marketplace participation

Table2: Notations used

Experimental Procedure

A total of 194 subjects from a North American university campus were the participants of the experiment. The subjects were randomly assigned to one of the cell. The procedure required the subject to visit a particular website based on the cell they were assigned to. Once a subject chose a product, she added the product to the cart and proceed with the checkout process. Subjects were asked to stop at the step when they have to provide their credit card information. At this point subjects had to close the browser and answer the provided questions on the instrument based on the perception s/he had developed towards the web vendor and its site.

Subject Background Information

The subjects of the experiment were graduate and undergraduate students of business school of a North American university. The total number of subjects was 194 and 184 of the responses were usable. On an average for each cell of the experiment 30 subjects were assigned.

A Chi-square analysis revealed no significant differences in gender, level of study, experience with internet, or online purchase experience among the groups. A one way ANOVA further revealed no significant differences between the groups in terms of age, number of years in university, or average time spent surfing the Internet.

Measures

The instrument i.e. the structured questionnaire consists of several parts. Each part was designed to investigate the factors described in the model and items in the instrument have been validated in the existing literature. In our scale development we have followed the recommendation by Straub, 1989 and Bagozzi and Philips, 1982. All the items were measured on a 7 point likert scale.

i. *Perceived Trustworthiness*: We measured perceived trustworthiness of a vendor using 9 Items of the scale proposed by McKnight, 2002.
ii. *Perceived Reputation*: We measured perceived reputation of a vendor using a 3 item scale from Jarvenpaa and Tractinsky,1999.
iii. *Perceived Security*: We measured perceived using the 9 items scale developed by Flavián and Guinalíu, 2006. While 3 of those items were originally proposed by Raganathan and Ganapathy, 2002,2003, others are proposed by Flavián and Guinalíu, 2006.

Manipulation Check

We performed several manipulation checks to make sure the experiment has been conducted appropriately. To ensure that companies categorized as less known companies in the experimental setup are really less known to the participants, we asked the participants regarding their familiarity with the web vendor. Almost none of the participants (less than 4%) had heard the name or visited the websites before. We did a one way ANOVA test to

find any significant difference in the familiarity of the web vendors among the participants. ANOVA analysis did not show any significant difference.

Before drawing inferences our data on the effect of third party payment mechanism, we had to make sure that the participants' perception towards the third party checkout is not significantly different. We conducted a one way ANOVA and it showed that there is no significant difference among the groups in terms their perception towards the third party payment mechanism. We noticed that in general the perceived trustworthiness of the third party payment mechanism i.e. Google checkout is high (Mean 6., SD .9)

We also had to make sure that the participants' perception towards the marketplace provider (in our case amazon.com) is not significantly different. We did a one way ANOVA and it revealed no significant difference between groups in terms of their perception towards the marketplace provider. We found that in general perceived trustworthiness of the marketplace provider i.e.amazon.com is very high (Mean 6.2, SD .8).

DATA ANALYSIS AND RESULT

To ensure the appropriateness of the research instrument, the data was statistically tested to assess the convergent validity, reliability, and discriminant validity of the scales. Based on the criteria mentioned in Nunnally,1994, Cronbach alphas for each measure (shown in the table4) indicated that construct reliability was acceptable i.e. more than or equal to .7. We employed a three-step sequence suggested by Chellappa and Pavlou (2002) to assess convergent and discriminant validity was employed. We conducted an exploratory factor analysis to detect high loadings on hypothesized factors and low cross-loadings. We set all eigenvalues to greater than unity, and the items were reduced to their principal constructs. We used Principal components analysis as the extraction method for confirmatory factor analysis with Varimax rotation.

Item	PT	PR	PS
PT1 *I believe that this web vendor would act in my best interest*	.86		
PT2 *If I required help, this web vendor would do its best to help me..*	.88		
PT3 *This web vendor is interested in my well-being, not just its own.*			
PT4 *This web vendor is truthful in its dealings with me..*	.81		
PT5 *I would characterize this web vendor as honest.*	.88		
PT6 *This web vendor would keep its commitments.*	.69		
PT7 *This web vendor is sincere and genuine.*	.84		
PT7 *This web vendor has ability to handle sales and transactions*	.80		
PT8 *This web vendor has sufficient expertise to do business on the internet*	.70		
PT9 *This web vendor has sufficient expertise to do business on the internet*	.87		
PR1 *This online vendor is well known*		.81	
PR2 *This online vendor has a bad reputation in the market*		.88	
PR3 *This online vendor has a good reputation in the market*		.81	
PS1 *I think this web site has mechanisms to ensure the safe transmission of its users' information*			.81
PS2 *I think this web site shows great concern for the security of any transaction*			.8
PS3 *I think this web site has sufficient technical capacity to ensure that no other organization will supplant its identity on the internet*			.88
PS4 *I think this web site has sufficient technical capacity to ensure that no other organization will supplant its identity on the internet*			,86
PS5 *I think this web site has sufficient technical capacity to ensure that no other organization will supplant its identity on the internet.*		.	.70
PS6 *I am sure of the identity of this web site when I establish Contact via the internet*			.8
PS7 *Think this web site has sufficient technical capacity to ensure that the data I send will not be intercepted by hacker*			.82
PS8 *When I send data to this web site, I am sure they cannot be modified by third party*			.80
PS9 *I think this web site has sufficient technical capacity to ensure that the data I send cannot be modified by a third party*			.86

Table3: Item and factor loading

All items in the same construct had high correlations and loaded on their hypothesized factors. Their estimates were also positive and significant, providing strong evidence of convergent validity (Bagozzi and Yi, 1988). In contrast, items of different constructs showed very low correlations and low cross-loadings (<0.4 level). These results rendered evidence of discriminant validity.

	Perceived Trust	Perceived Reputation	Perceived Security	Cronbach's Alpha
Perceived Trust	1.0			.915
Perceived Reputation	.2693	1.0		.868
Perceived Security	.54	.64	1.0	.833

Table4: Reliability and covariance matrix

Hypotheses Testing

As hypothesized, we wanted to test whether there is a significant difference in perceived security of the control cells and the treatment cells attributable to the presence of trust transference mechanism. To compare the perceived security of two cells (i.e. control and treatment) and to test the proposed hypotheses, we used t-tests. The result of the t-tests has been presented in the table5.

Hypothesis	Result
H1a.(i.e. $PS_{(LKHS)} < PS_{(LKHSG)}$)	Not Supported(P>.01)
H1b.(i.e. $PS_{(LKLS)} < PS_{(LKLSG)}$)	Not Supported(P>.01)
H2a(i.e. $PS_{(LKHS)} < PS_{(LKHSM)}$)	Supported(P<.01)
H2b.(i.e. $PS_{(LKLS)} < PS_{(LKLSM)}$)	Supported(P<.001)

Table5: Hypotheses Testing Result

In order to test hypothesis H1a we have compared $PS_{(LKHS)}$ and $PS_{(LKHSG)}$ using t-test. The t-test did not reveal any significant difference (P>.01). Therefore, H2a has been rejected. Similarly, H1b has been tested applying t-test on $PS_{(LKLS)}$ and $PS_{(LKLSG)}$. The result of this t-test did not show any significant difference either (P>.01). Therefore, H1b has also got rejected.

In order to test H2a and H2b, once again t-tests have been applied. Result of t- test showed that there is a significant difference between $PS_{(LKHS)}$ and $PS_{(LKHSM)}$ (P<.01) suggesting that $PS_{(LKHS)}$ is significantly lower than $PS_{(LKHSM)}$. The result of t-test also showed that there is a significant difference in the between $PS_{(LKLS)}$ and $PS_{(LKLSM)}$ (P<.001) suggesting that $PS_{(LKLS)}$ is significantly lower than $PS_{(LKLSM)}$. Hence, based on these two t-tests we can conclude that both hypothesis H2a and H2b have got supported.

DISCUSSION OF RESULTS

The result of our experiment showed that an electronic marketplace is an effective trust transference mechanism while a third party checkout is not. It is interesting to that there was no significant difference in the perceived security towards the less known web vendors unless they participate on marketplace as a mean to gain transference based trust.

In general, perceived security towards a less known vendor with highly visible security features (Mean 4.8,SD. 6) was little higher than the a less known vendor with less visible security features(Mean 4.5,SD. 6). It is interesting to notice that difference is not statistically significant (P>.01). There was also no significant difference perceived security towards a less known vendor with highly visible security features and third party checkout (Mean 4.6,SD. 6) and a less known vendor with less visible security features and third party checkout (Mean 4.4,SD. 5). It is also

interesting to notice that there was no significant difference in the perceived security towards a web vendor with highly visible security features (Mean 6.1, SD .5) and perceived security towards a web vendor with less visible security features(Mean 6, SD .5) if both of them were participating on marketplace. In general, perceived security towards the web vendor participating on a marketplace was significantly higher than the companies those are not.

This finding is consistent with the concept of "entitativity" introduced by Campbell (1958). He suggested that trust transfer from one entity to another relies on the unknown target being perceived as related to the source of the transferred trust. Campbell (1958) suggested that such perceptions are developed upon the similarity, proximity, and common fate of the entities. The term "entitativity" means the degree to which a collection of individuals is perceived as forming a group. Stewart (2003) found the higher the level of entitativity, the more effective trust transference is. This finding by Stewart (2003) explains the reason of our experimental result. The way third party checkout mechanism works, it does not show a higher level of entitativity to a potential customer. The customers only get to see the third party checkout system after they have added something on the cart and planning to checkout. Hence, by that time a customer has already created a perception towards the web vendor and its security mechanism. Therefore, the level of entitativity is low for the third party checkout mechanism, so is the trust transference. Whereas, in the case of marketplace, a customer interacts with a web vendor on the very platform marketplace provides which presents a higher level of entitativity between the less known web vendor and the trusted marketplace. This higher level of entitativity makes trust transference mechanism effective and a less known web vendor gains a higher level of perceived security.

Perceived security of the customers is one of the major obstacles a relatively new web vendor has to face in order to be successful. In order to achieve that management of a company decides to spend resource (e.g. money, manpower) on certain techniques like associating with a trusted third party or placing security mechanisms on the website. The findings of our study suggest that participating on a marketplace is the best strategy of achieving higher perceived security for a less known web vendor.

CONCLUSION

The primary contribution of this research is to introduce trust transference as a mean to gain higher perceived security for the less known companies and empirically test the effectiveness of two trust transference mechanisms. Our result showed that while due to entitativity, marketplace was an effective trust transference mechanism, third party checkout was not. Our result also showed that in terms of getting higher perceived security of the customers, participating on a marketplace is the most suitable strategy for a less known company.

In this paper we have focused only on the less known companies who lack reputation in the current market. However, in future we intend to empirically test effectiveness of the trust transference mechanisms for both well known and less known companies. The concept of trust has been three major dimensions- benevolence, integrity and competence (McKnight et al, 2002). One interesting future research direction would be to examine the effectiveness of trust transference mechanism on each of those three dimensions.

REFERENCES

Ahuja, M., Gupta, B. , Raman, P.,(2003) An Empirical Investigation of Online Consumer Purchasing Behavior, *Communication of ACM*, 46 (12ve), 145-151.

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall.

Bakos, Y ,1998. The emerging role of electronic marketplaces on the Internet. *Communication of ACM* 41, 8, 35–42.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems*, 11, 245–270

Campbell, D. T. 1958. Common Fate, Similarity, and Other Indices of the Status of Aggregates of Persons As Social Entities. *Behavioral Science* **3** 14-25

Casalo, L. V. (2007)The Influence of Satisfaction, Perceived Reputation and Trust on a Consumer's Commitment to a Website, *Journal of Marketing Communications* (13:1), 2007, pp. 1-17

Chellappa, R., P. A. Pavlou. 2002. Perceived information security,financial liability, and consumer trust in electronic commerce transactions. *J. Logist. Inform. Management* 15(5–6) 358–368.
Chiles, T. H., & McMackin, J. F. (1996). Integrating variable risk preferences, trust, and transaction cost economics. *Academy of Management Review*, 21, 73-99.
Chou, D., Yen, D., Lin, B. and Hong-Lam Cheng, P. (1999), Cyberspace security management, *Industrial Management & Data Systems*, Vol. 99 No. 8, pp. 353-61.
Cranor, L. F. , Reagle, J., Ackerman, M. S. (1999) Beyond Concern: Understanding Net Users' Attitudes about Online Privacy, *AT&T Labs-Research Technical Report*.
Doney, P. M., and Cannon, J. P. (1997) An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing*, 61, 35-51.
Dong-Her, S., Hsiu-Sen,C. Chun-Yuan, B Lin (2004) Internet security: malicious e-mails detection and protection, *Industrial Management and Data Systems*, Volume:104 Issue:7
Flavián, C. Guinalíu , M .(2006) Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site, *Industrial Management & Data Systems*
Heider, F. (1958)The Psychology of Interpersonal Relations, New York: John Wiley and Sons,
Hosmer, L., (1995)Trust: the connecting link between organizational theory and philosophical ethics. *Academy of Management Review* 20, 379–403.
Jarvenpaa, S. and Tractinsky, N. ,(1999) Consumer Trust in an Internet Store: A Cross-Cultural Validation", *JCMC* 5 (2) December
Kim, D.J. Steinfield C and Lai Y(2004) Revisiting the Role of Web Assurance Seals in Consumer Trust, *Proc. of the 6th international conference on Electronic Commerce*, pp.280-287 (2004)
Kovar, S. E, Burke K. , Kovar , B. (2000) Consumer Perceptions of CPA WebTrust Assurances: Evidence of an Expectation Gap, *International Journal of Auditing*, 3, 2000, 89-105.
Latour A, (1999) PayPal Electronic Plan May be On the Money in Years to Come, *The Wall Street Journal Interactive Edition*, Nov
Jøsang A, Ismail R, Boyd C,A Survey of Trust and Reputation Systems for Online Service Provision", *Working Paper*
Kalakota, R., Whinston, A.B.(1996), Frontiers of Electronic Commerce, Addison-Wesley, Reading,
Mayer, R.C.; Davis, J.H. and Schoorman, F.D.(1995) An integrative model of organizational trust,. *Academy of Management Review*, ,Vol20, No.3 pp709–734.
McKnight H. Choudhury V., Kacmar C., (2002) Developing and Validating Trust Measures for e-Commerce: An Integrative Typology, *Information Systems Research*, Informs Vol. 13, No. 3, pp. 334-359
McKnight, D. H., Cummings, L. L. and Chervany, N. L.,(1998) Initial Trust Formation in New Organizational Relationships. *Academy of Management Review* (23:3), pp. 473–490.
Milliman, R. E. and Fugate, D. L. 1988. Using Trust-Transference As a Persuasion Technique: An Empirical Field Investigation. *Journal of Personal Selling and Sales Management* 1-7
Noteberg, A., Christaanse, E., Wallage, P.(1999)The Role of Trust and Assurance Services in Electronic Channels: An Exploratory Study, *presented at The Twentieth International Conference on Information Systems*, Charlotte, North Carolina, 1999.
Nunnally, J.C., Bernstein, I. H. (1994) Psychometric Theory, 3rd ed. New York: McGraw-Hill.
Raykov, T. & Marocoulides, G. A. (2000). *A First Course in Structural Equation Modeling, 2nd Edition*. Mahwah, NJ: Lawrence Erlbaum Associates
Ranganathan, C. and Ganapathy, S. (2002), Key dimensions of B2C websites, *Information & Management*, Vol. 39, pp. 457-65.
Salam, A.F., Iyer, L., Palvia, P., and Singh, R. (2005)Trust in E-Commerce. Communications of the ACM. Vol. 48, No. 2, pp. 73-77
Soh, C., Markus, L., Goh, K. H.,(1998) Electronic Marketplaces and Price Transparency: Strategy, Information, Technology and Success, *MIS Quarterly*(30:3), 1998,
Stewart, Katherine J.(1999)Transference as a Means of Building Trust in World Wide Web Sites in the *Proceedings of the 20th International Conference on Information Systems* in Charlotte, NC.
Stewart, KJ(2003) Trust Transfer on the World Wide Web *Organization Science*,Vol14No1
Suh, Bomil and Han, I. *The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce*, International Journal of Electronic Commerce ,Volume 7, Number 3 / Spring 2003,135 - 161
Turner Carl W., Zavod, M., and Yurcik, W. (2001) Factors that affect the perception of security and privacy of e-commerce web sites. *Proceedings of the Fourth International Conference on Electronic Commerce Research* Vol. 2, pp. 628-636.

Wang, H., Lee, M.K.O., Wang, C.(1998)Consumer privacy concerns about internet marketing, *Communications of the ACM* 41 (3), 63–70.
Wixom, B. H., Watson, H. J. (2001) An Empirical Investigation of the Factors Affecting Data Warehousing, *MIS Quarterly*, 25 (1), 2001, 17-41.
Yenisey, Ozok A, Salvendy G(2005) Perceived security determinants in e-commerce among Turkish students. *Behavior & Information Technology* (Print) 24:44, 259-274, Taylor & Francis,