Journal of Information Technology Management

ISSN #1042-1319

A Publication of the Association of Management

MODELING USER PERCEPTIONS OF E-COMMERCE SECURITY USING PARTIAL LEAST SQUARE

MOHANAD HALAWEH
UNIVERSITY OF DUBAI
mhalaweh@ud.ac.ae

ABSTRACT

Previous research has shown that perceived security has an influence on customers' acceptance of e-commerce and intention to purchase online. However, little research investigates the antecedent factors that influence that construct (i.e. perceived security). This paper aims to predict and test the factors that influence the customer's perception of e-commerce security. A research model of the influencing factors was developed based on qualitative research data. This led to formulating five hypotheses. A survey was designed to collect data and test the hypotheses using the partial least squares (PLS) approach. The results supported three out of the five hypotheses of this study that user characteristics, psychological state and intangible security features demonstrated a significant influence on the level of perceived e-commerce security. The research implications for practice and future research are also discussed.

Keywords: e-commerce, security, security perception, partial least squares (PLS)

INTRODUCTION

Security is a constant challenge for the acceptance and adoption of e-commerce. This was confirmed by the Kikscore survey that was conducted through the USA in August 2011. It showed that 90% of online customers did not complete a transaction online because of fear of being defrauded or being a victim of online scam [26]. Previous research studies have also shown that customers' positive perception of security is an essential pre-requisite to their willingness to engage in online transactions [8, 13, 14]. However, little research attempts to find out the antecedent factors that have an impact on security perception. This paper builds on earlier work carried out by Halaweh [9], which identified, based on explorative qualitative research, the factors/issues that influence customers' perception of e-commerce security. Although qualitative research methods were appropriate to investigate the research problem in depth and collect intensive data from the research participants, data were collected through interviews from a small number of participants. This makes it impossible to generalise the results and statistically investigate the significance of the factors and relationship between them. Thus, this research moves one step forward to establish a model of factors that influence the perception of e-commerce security and formulates a set of hypotheses with the aim of testing them statistically using the PLS approach to structural equation modeling.

The remainder of this paper is organised as follows: Section 2 presents a literature review that summarises earlier contributions. Section 3 presents the research model and hypothesis. Section 4 presents the research methods. Section 5 provides a discussion and practical implications. Finally, the research conclusion is provided.

LITERATURE REVIEW

Yenisey et al. [25] defined perceived security as the level of security that customers feel while they are shopping on e-commerce websites. Salisbury et al. [16] defined perceived Web security as the extent to which customers believe that the Web is secure for transmitting sensitive information such as credit card details. Lallmahamood [14] provided another definition, stating that perceived security is the users' perception of protection against security threats and control of their personal information in online applications. He adds that it is about a user's self-belief in the system to perform a transaction securely. In addition, Chellappa and Pavlou [2] defined perceived security as the subjective probability with which customers believe that their personal information will not be accessed or manipulated during a transaction by unauthorised parties, in a way that is consistent with their confident expectations. It can be said and based on all previous definitions that perceived security is the subjective feeling and belief of e-commerce customers that their personal information is protected against any threats when they carry out online transactions. Threat sources can be a business operating e-commerce that does not implement the best security technology standards, a company that misuses customer information, threats that customers face as a result of the loss of control and encountering complexity in e-commerce interfaces, threats that can also happen through external sources by hackers who run fake and phishing e-commerce interfaces. Furthermore, customers themselves are a source of threat; they increase the level of risk if they are not aware of security measures, and do not know exactly how to protect their personal data. In summary, they refer to any threats that make users feel and believe that their private information is unsecure.

The contribution of previous research showed a set of factors and features that influence customers' perception of security such as ease of use, a site's visual appeal, effective interface design, authentication mechanisms (e.g. using PIN numbers), and third-party trust symbols like VeriSign, a third-party privacy seal like TRUSTe, the presence of data encryption (as indicated by <https> in the browser address, padlock icon, privacy and security policy statements, demos and frequently asked questions (FAQs) [17, 18, 22, 23, 25]. The research also provides evidence of the impact of the perception of security on the adoption and trust of e-commerce. Table 1 shows a sample of articles examined and reviewed on security perception and its influence on e-commerce acceptance.

Table 1: Sample of Existing Literature in E-commerce Security Perception

	Authors	**Contribution**
1	Salisbury et al. [16]	Providing evidence of impact of Web security perception on the intention to purchase online
2	Chellappa and Pavlou [2]	Showing that perceived privacy and security are the main determinants of trust in e-commerce transactions
3	Suh and Han [19]	Identifying and showing the impact of customers' perceptions of security controls (non-repudiation, privacy protection and data integrity) on trust and e-commerce acceptance
4	Yenisey et al. [25]	Identifying factors influencing customers' perceptions of security in e-commerce
5	Singh [18]	Showing evidence that ease of use, convenience, usefulness and the ability to control increase customers' perceptions of security in online banking
6	Connolly and Bannister [5]	Studying the impact of perceptions of security control on trust in Internet shopping
7	Ha and Stoel [8]	A structural equation model was used to demonstrate that shopping enjoyment and perceived security and trust play significant roles in the consumer adoption of e-commerce
8	Khasawneh et al. [12]	A survey was conducted to showcase that security issues are major barriers to Internet banking and e-commerce
9	Catharina and Paradice [1]	A study showed that the use of security symbols and trustworthy brand names have a positive effect on trusting e-commerce
10	Kim et al. [13]	An empirical study showed that perceived security and perceived trust have a strong impact on the use of e-payment systems

The current research adds to the existing literature in at least two aspects. Firstly, most of the previous research attempts to prove that perceived security has a significant influence on e-commerce adoption and the intention to purchase online. This research moves one step backward to investigate the antecedent factors that have an impact on e-commerce security perception. Secondly, this paper develops a research model of factors (based on qualitative data analysis) that influence e-commerce security perception from a wider perspective, more than security features or symbols (which represent one construct in the study), as shown by most previous studies [17, 18, 25]. The research model contains wide issues and unique constructs such as the psychological state of security, cooperative responsibility and other factors, as will be shown in the next section, which are proposed for testing for the first time.

RESEARCH MODEL AND HYPOTHESIS

The model of factors and their relationships with the perception of e-commerce security is set out in Figure 1, which reveals the five constructs' effect on e-commerce security perception. The model was developed to test the validity of the hypotheses that emerged from the exploratory qualitative study. These constructs are explained in the following paragraphs.

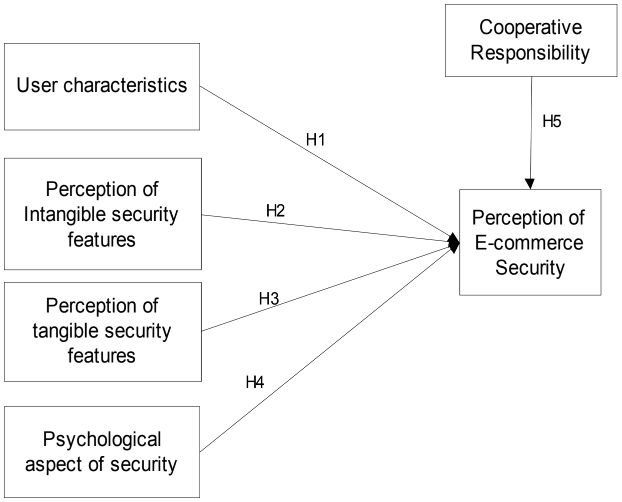
Cooperative Responsibility
User characteristics
H1
H5
Perception of Intangible security features
H2
Perception of E-commerce Security
Perception of tangible security features
H3
H4
Psychological aspect of security

Figure 1: Proposed Theoretical Model with Hypotheses

User Characteristics

Users have varying levels of security awareness characterised by their experience, knowledge and willingness to experiment. The concepts of experience, knowledge and practice concern the means of dealing with the website and what must be known in order to determine whether that website is secure. Some users/customers may have no knowledge of security issues and buying online: some have no understanding of the meaning of security features on e-commerce websites (e.g. the padlock symbol, (s) in https), so they depend on the experience of others. The level of each concept differs from one customer to another. A user who has a high level of experience and knowledge tends to use e-commerce with confidence, whereas other users will not engage in this activity. Some users gain knowledge and experience by time and practice. Some users do not know what they should and show their continuous learning of new things. It is clear that differences exist between the concepts that represent user characteristics; for example, learning is the process of obtaining knowledge, and utilising this knowledge in reality can be called practice or experimentation. However, the main difference between them is that experimentation might occur without any prior knowledge, perhaps by chance or through the user's curiosity to try something new. Repeating practice and experimentation many times creates experience. It was noted that some users clearly had no knowledge of security or even online buying. Some were learning, others claimed to have some knowledge, while some believed they had experience after their first experimentation by curiosity. Thus, it is expected that:

H1. Users' characteristics will positively influence their perception of e-commerce security

Perception of Tangible and Intangible Security Features

Tangible indicators are those technological security features of websites that can be checked by users, such as https, padlocks and security certificates, whereas intangible ones (e.g. famous website, reputation) are not seen on the website and cannot be directly checked over the website. They are affected by society in terms of communication and the environment: where the customer lives and what they hear from others, as well as their past experience. Tangible features need to be understood and checked by the customer over the website rather than captured through social communication; this involves having knowledge and experience of these features, such as knowing what a security certificate means and how to check whether it has expired. Thus, it is expected that:

H2. Users' perception of intangible security features will positively influence their perception of e-commerce security

H3. Users' perception of tangible security features will positively influence their perception of e-commerce security

The Psychological Aspect of Security

The psychological aspect of security incorporates the feeling of fear, the need to feel that one's money is secure, and the ability to control the payment process and performance of online transactions. Many customers have the misconception that the use of e-commerce for buying and selling is vulnerable and that there is a high probability that their money will be lost. This is due to the intrinsic nature of e-commerce, being remote rather than face-to-face. Therefore, the user does not touch or see anything except the computer screen; what lies behind this screen is unknown, and this makes consumers very skeptical. Thus:

H4. Users' psychological state will negatively affect their perception of e-commerce security

Cooperative Responsibility

Cooperative responsibility means that the success of e-commerce in terms of security involves the responsibility of different actors who complement each other, rather than a single responsibility. The responsibility for security insurance is initially undertaken by the users themselves, and that part of this responsibility is generally outlined on the selling company's website. Businesses engaging in e-commerce have a responsibility to develop secure websites by adopting the best technology and providing the required security conditions. They exercise this responsibility through their sites' security features, the security materials published on the sites, and by providing brief security explanations and checklists of important security points. Part of this responsibility lies in management's commitment to the necessary expenditure on security. Websites that present such information to their users so that they can verify it before conducting their transactions encourage users to feel that the companies are committed to their customers' security. In essence, part of the company's responsibility is to protect its customers' data. Companies that implement the latest security technology to ensure the security but misuse and abuse their customers' data once it is stored in their databases are responsible and accountable for security violations. There is also cooperative responsibility by the government and banks toward the implementation concerns. The government can play a major role in e-commerce security by providing a secure national electronic payment gateway that enables companies to securely run their business through it. It is the education system's responsibility to increase individual awareness and perception by enriching people's knowledge and experience of security and the use of e-commerce, as well as propagating a culture of using e-services to carry out activities online. The banks also have an important role in providing customer facilities for credit/debit cards and by issuing cards for limited amounts. This enables customers to use them for shopping online, thus reducing the level of potential risk. Thus:

H5. Cooperative responsibility will positively influence users' perception of e-commerce security through cooperation between the involved entities

RESEARCH METHODOLOGY

This research project was divided into two stages: 1) investigating the themes/factors/issues that influence security perception from the customer perspective using qualitative research methods (interviews), which resulted in the publication journal paper [9]. The second stage reflects the purpose of this paper, which is to generate a model of factors that influence customers' perception of security, and test it using quantitative methods to determine the significance of the identified factors and their influence. Thus, a set of hypotheses were formulated, as presented in the previous section. A survey instrument was also designed, as shown in Table 2. The survey items used to measure the research model constructs were primarily derived from the qualitative data. All items are assessed by a five-point Likert scale. A survey was distributed to 68 students who registered in the MIS course. A total of 61 participants filled out and returned the survey. The data was analysed using partial least squares (PLS) with SmartPLS software [20]. PLS is a form of component-based structural equation modeling, which is frequently used in IS research [7, 24]. PLS is typically recommended in situations in which there are no stable, well-defined theories to be tested in a confirmatory research setting, when the objective is prediction, and when the sample size is small [4, 10; 24]. For all these reasons, PLS was the appropriate approach for this research. The model of factors and relationships (depicted in Figure 1) was developed based on qualitative data. Hence, it is still not well-established theory, as it contains constructs that were not previously tested. The research also aims to predict the significance of the relationship hypothesised in the previous section. In addition, the sample size is conformable to the PLS technique. Furthermore, the condition of minimum sample size was met, as Chin [3] proposed, in which the minimum sample size should be ten times the largest number of structural paths directed at a particular latent construct in the structural model. The research model (Figure 1 or 2) has only one dependent (latent) variable, namely "perceived e-commerce security", which has five paths directed to it. Thus, the sample size of this study should be a minimum of 50, and this has been met (the sample is 61).

Table 2: Survey Constructs and Measurements

Construct		**Item**
User/customer characteristics (UC)	UC1 UC2 UC3	I rely on my past experience when I shop online I have enough knowledge to shop online I rely on experiment when I shop online
Cooperative responsibility (CR)	CR1 CR2	I think security insurance in online shopping website is a mutual responsibility I think security insurance in online shopping website is a responsibility that involves several entities such as the e-commerce website company, e-commerce users, financial sectors (bank), media, and universities
Psychological aspect of security (PS)	PS1 PS2 PS3	I fear when I shop online I sometimes have misconceptions about shopping online I feel anxious to shop online because of the nature of e-commerce, which involves a lack of face-to-face communication
Tangible features security (TS)	TS1 TS2 TS3	I check the presences of http(s) in the URL when I shop online I check the small padlock icon on the bottom right corner of the website when I shop online I check the digital security certificate of the website when I shop online
Intangible indicators of security (IS)	IS1 IS2 IS3 IS4	I would shop online on a reputable website I would shop online on a local website I would shop online on a click and mortar website (i.e. company has online and offline stores) I would shop online on a website that provides contact information (telephone, email, fax)
Perceived e-commerce security (PES)	PES1 PES2	I believe shopping online is secure Online shopping websites give me a feeling of security

RESEARCH RESULTS

The following paragraphs assess the measurement model and structural equation model.

Measurement Assessment

The measurement model was assessed by reliability, convergent and discriminant validity. Reliability was tested by Cronbach's alpha. According to Hair et al. [11], items have acceptable reliability if the Cronbach's alpha value is greater than 0.6 and high reliability if the Cronbach's alpha value is greater than 0.7. Table 3 shows that the Cronbach's alpha value of cooperative responsibility is slightly lower than 0.7 (0.679), which is acceptable, while the remainders are greater than 0.7. This means that those constructs have high reliability.

The convergent validity was assessed by factor loadings, composite reliability and average variance extracted (AVE). The loadings for all items exceeded the recommended value of 0.6 (see Table 4). All of the constructs exceeded the threshold for composite reliability, as they were greater than 0.70 [11] (see Table 4), ranging from 0.837 to 0.918. All values of average variance extracted were higher than 0.5 [11], ranging from 0.634 to 0.850. Table 3 provides a summary of reliability and convergent validity.

Table 3: Summary of Reliability and Convergent Validity

	Cronbach's Alpha	AVE	Composite Reliability
Cooperative Responsibility	0.679	0.733	0.844
Intangible Security Features	0.834	0.669	0.889
Perceived E-commerce Security	0.824	0.850	0.918
Psychological State	0.812	0.715	0.881
Tangible Security Features	0.857	0.762	0.905
User Characteristics	0.705	0.634	0.837

Table 4: Item Loading

Construct	Items	Factor Loading
Cooperative Responsibility	CR1_7	0.743
	CR2_8	0.955
Intangible Security Features	IS1_16	0.713
	IS2_17	0.892
	IS3_18	0.907
	IS4_19	0.742
Perceived E-commerce Security	PES1_20	0.930
	PES2_21	0.913
Psychological State	PS1_9	0.904
	PS2_10	0.686
	PS3_11	0.925
Tangible Security Features	TS1_13	0.751
	TS2_14	0.954
	TS3_15	0.901
User Characteristics	UC1_1	0.873
	UC2_2	0.822
	UC3_3	0.680

Discriminant validity was assessed by examining whether the square root of AVE for each construct was higher than the squared correlation between that construct and all other constructs [6]. Table 5 shows that discriminant validity was met. It can be seen that the square root of the AVE for each construct was greater than the correlation between constructs. As a result, the measurement model demonstrated adequate reliability, convergent validity and discriminant validity.

Table 5: Correlation between Constructs
(diagonal represents the square roots of average variance extracted)

	Cooperative Responsibility	Intangible Security Features	Perceived E-commerce Security	Psychological State	Tangible Security Features	User Characteristics
Cooperative Responsibility	**0.856**					
Intangible Security Features	0.356121	**0.817**				
Perceived E-commerce Security	0.250008	0.423776	**0.921**			
Psychological State	-0.114560	0.022648	-0.343490	**0.845**		
Tangible Security Features	0.154357	0.452951	0.273722	-0.142208	**0.872**	
User Characteristics	0.328931	0.450597	0.513096	-0.119308	0.363029	**0.796**

Structure Equation Model

Two measures were used to assess the structural model: the statistical significance (t-tests) of the estimated path coefficients, and the ability of the model to explain the variance in the dependent variables (R square). R square attempts to measure the explained variance of the dependent variable relative to its total variance. Values of approximately 0.670 are considered substantial, values around 0.333 moderate, and values of approximately 0.190 weak [3]. The R square of the research model was 0.403, indicating that 40 per cent of the variance in perceived e-commerce security was explained by the independent variables, which is moderate variance. Figure 2 shows the R square for the dependent variable (perceived e-commerce security). To test the significance of the hypotheses, rule proposed by Martinez-Ruiz and Aluja-Banet [15] was followed. The t-value >1.65 is significant at the 0.05 level, and the t-value > 2 is significant at the 0.01 level. Table 6 and Figure 3 show the t-value for each hypothesis and indicator. Only three of the five hypotheses were supported. User characteristics, psychological state, and intangible security features demonstrated a significant influence on the level of perceived e-commerce security. Therefore, hypothesis H1, H2 and H4 were supported.

Cooperative responsibility and tangible security features did not demonstrate a significant influence on the level of perceived e-commerce security. Therefore, hypotheses H3 and H5 were not supported.

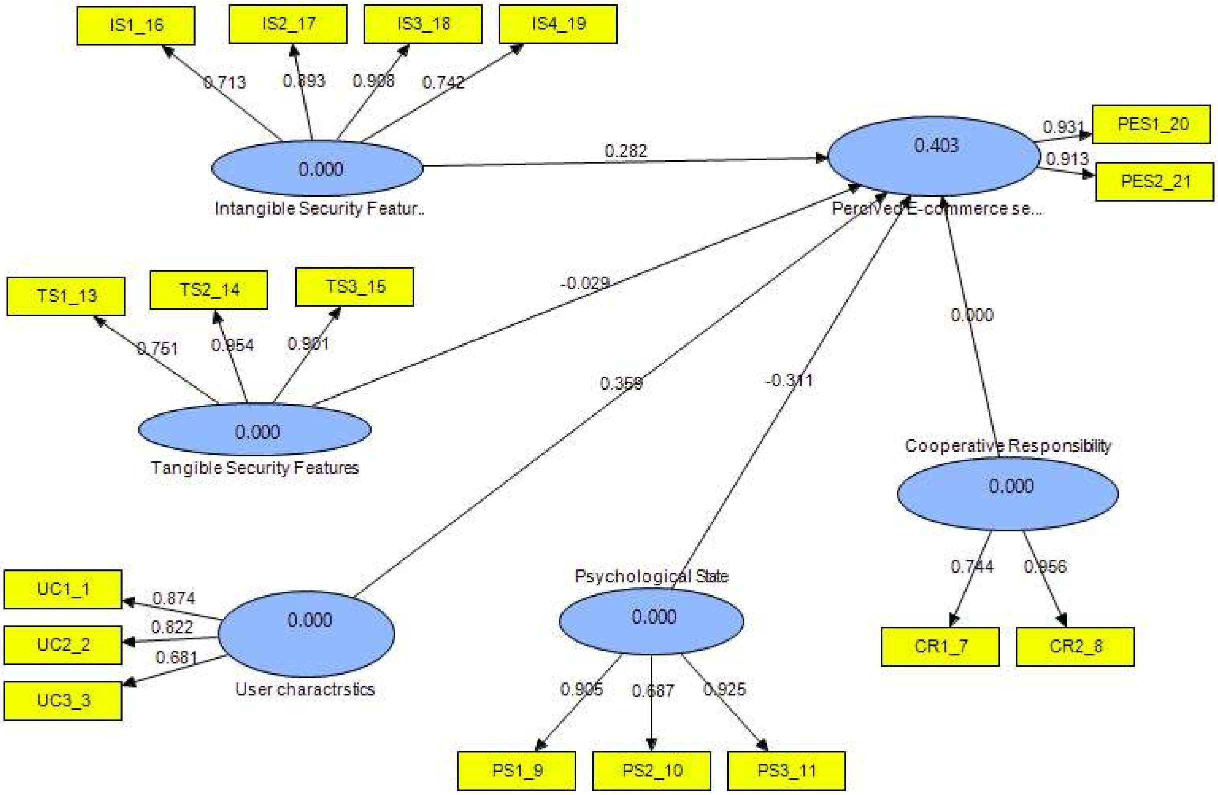

Figure 2: PLS Structural Equation Model

Table 6: Hypothesis Testing Based on T-values

H no.	Hypothesis	T Statistics	Significance
H1	**User characteristics -> Perceived e-commerce security**	2.537172	Supported *
H2	**Intangible Security Features -> Perceived e-commerce security**	1.910924	Supported **
H3	**Tangible Security Features -> Perceived e-commerce security**	0.196634	Not Supported
H4	**Psychological State -> Perceived e-commerce security**	2.657917	Supported *
H5	**Cooperative Responsibility -> Perceived e-commerce security**	0.001875	Not Supported

Note: t-value >1.65 is significant at the 0.05** level; t-value > 2 is significant at the 0.01* level

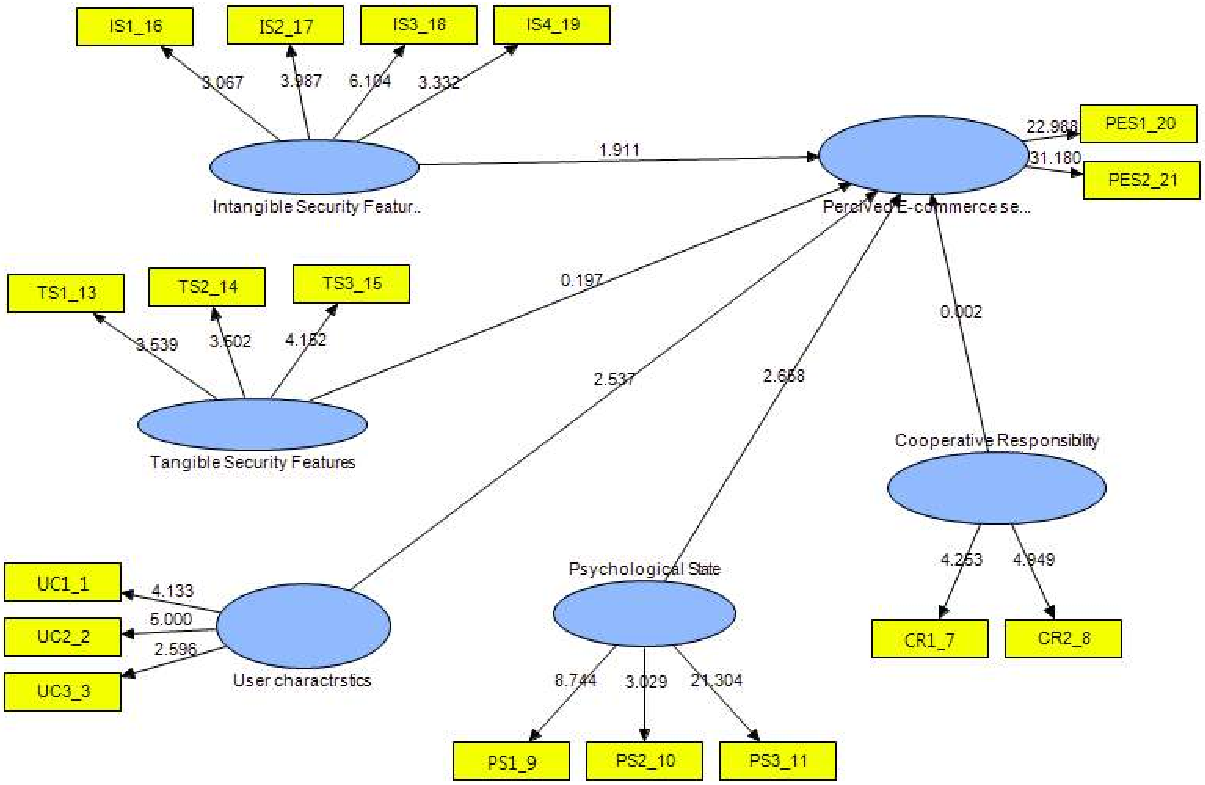

Figure 3: Factors Relationship with Perceived E-commerce Security by T-values Using SmartPLS

DISCUSSION AND RESEARCH IMPLICATIONS

The study was conducted to predict the antecedent factors that have an influence on customers' perception of e-commerce security. The results show that user characteristics, psychological state and intangible security features have an influence on their security perception. Regarding the user characteristics factor, the designer of e-commerce websites should take into consideration that the amount of security information and tips needs to be customised and personalised according to the users' level of knowledge and experience. For example, the designer can provide a link in the interface for first-time users who would like to pay online by using a credit card just before starting the transaction to guide them about what they have to check and how to complete the transaction securely without any complexity. If the user is already familiar with the online payment process, he/she can skip this step. Some websites provide security tips, but this information is usually placed in a separate Web interface and not integrated with the payment process-related interfaces (i.e. not contextual). Therefore, it is supposed that is the user's responsibility to visit that webpage and read about the security instructions. However, in the second approach, the security tips are customised/ personalised based on the user's knowledge level and provided when the user launches the payment transaction. This enables users to learn and be aware of security instructions and positively increases their security perception of the e-commerce website.

The research findings show that there is a strong correlation between the psychological state of security and customers' perception of e-commerce security. In fact, the psychological state concerns the feeling of fear and anxiety, which the customer may have experienced before, during and after online purchasing. For example, when the media disseminates a negative picture of the use of e-commerce through the propagation of negative news stories about stolen money and online fraud, it causes customers to become fearful and instills a reluctance to use e-commerce. Thus, this constitutes a misconception about e-commerce security before deciding to purchase online.

During the purchasing process, the customer may also experience anxiety due to the complexity of the interface design and a feeling of being lost. After purchasing, the customer may have to wait a couple of days to a week to have the product delivered. Thus, he or she will be worried until receiving the product and ensuring that it is actually the requested product. To alleviate the psychological feeling, the media (through different channels and levels) plays a major role in not overemphasising the fraud stories, and by contributing in raising consciousness amongst users of what security instructions and tips need to be checked and practiced in order to reduce their feeling of fear. For the second point, user interface (UI) designers play a major role in designing usable interfaces that promote security awareness and give customers a sense of safety. In this regard, it is recommended for future research to develop a set of guidelines that can be followed by UI designers, which reflect the meaning of security (security design). Guidelines are more than symbols placed on the website like checking for a padlock or placing Versign icons on the interface. Rather, focusing on every aspect of the design can contribute to designing e-commerce interfaces that are not complex, do not cause customers anxiety, and give them a sense of security. For the last point, the psychological feelings that affect the user due to the nature of e-commerce, which are related to anonymity and the absence of face-to-face interaction, the e-commerce website needs to guarantee a refund if the customer does not like the product and present some information on the website that asserts this point, taking into consideration that the customer has to pay before receiving the product (i.e. in the case of physical goods). E-commerce websites can also provide a security resolution centre to solve the problems faced by customers, especially ones that affect their psychological state. It is also important to use that label (security resolution centre) instead of customer service, as the name relieves the customer of worries related to all security concerns, before, during and after online purchasing.

The research findings also show that the tangible security features (e.g. security certificate) of e-commerce do not play a role in user's perception of e-commerce security. However, this result can be interpreted in that the participants do not understand exactly what these indicators mean and how to check them on the website. Conversely, intangible features influence customers' perception of security. In fact, these features (e.g. famous website, reputation) are identical to some factors that influence trusting a website (such as reputation) [5, 21]. However, this suggests that users prefer to deal with a trusted website, and this impulsively guarantees that they deal with a secure website. For example, Amazon is a well-known and reputable website, so it is believed to be trustable. Thus, not everyone checks the tangible security features on the Amazon website because some customers believe that the reputation of the website implicitly insures security. However, not every trusted website is secure. For example, citizens might trust an e-government services website. However, this does not necessarily mean that the government has applied the best security technology to protect the data of citizens. Moreover, one may purchase from a secure website that has applied the best security technology, but the company that owns the website may use the customer data once it is stored in their database for marketing purposes or sell it to a third party. Therefore, the security violation comes from the website itself as a result of misuse even though the data is secured through the transmission by encryption. On the other hand, consumers sometimes encounter websites whose identity is unknown or unfamiliar, but they still purchase from them by checking the security features such as a padlock and security certificate. Thus, for users, both tangible and intangible security features need to be examined. E-commerce companies need to work on them together in order to positively increase customers' perception of security.

Finally, regarding the cooperative responsibility construct, the findings show that customers do not believe that their perception of e-commerce security is a mutual responsibility between themselves, the e-commerce website and other entities. In essence, this factor was not tested before, as it was revealed only by the analysed qualitative data. However, this partially conforms to an earlier study by Turner et al. [22]. They found, based on the viewpoint of security experts, that security should be the responsibility of the customer and that customers need to ensure their own security by protecting their passwords and credit card numbers. This means that customers themselves can raise and minimise this risk, irrespective of which website they visit. Nonetheless, this does not exempt e-commerce websites from assuming responsibility for protecting customer data, designing usable interfaces, and providing the required security instructions and tips on their e-commerce websites.

CONCLUSION

This paper has made a theoretical contribution by establishing the factors that influence e-commerce security perception from the customer perspective. The research results show that user characteristics, psychological state and intangible security features have a significant influence on e-commerce security perception. In contrast, tangible security features and cooperative responsibility have a non-significant influence. Although using survey instruments and hypotheses testing by PLS enabled the author to prove the significance of three antecedent factors (three hypotheses), the research results might differ if the data was collected from another context with a larger sample size.

For practitioners, this research provides organisations that intend to run their business via e-commerce with a way of thinking about this extensively by considering several technical and non-technical factors. Therefore, it is necessary to establish which factors should be considered in order to guarantee that security is perceived positively. The previous section provided implications for e-commerce designers and decision makers to deal with these influencing factors.

One limitation of this study is the sample size, which was relatively small, and the fact that the data collection only took place amongst MIS students. Although it has been justified that the sample size is suitable for the PLS technique, a further investigation of these described constructs and hypotheses in a different context can help to generalise the results.

REFERENCES

[1] Catharina, M. and Paradice, D. B. “An Examination of the Impacts of Brand Equity, Security, and Personalization on Trust Processes in an E Commerce Environment*”, Journal of Organizational and End User Computing*, Volume 21, Number 1, 2009, pp. 1-36.

[2] Chellappa, R. k. and Pavlou, P. A. “Perceived information security, financial liability and consumer trust in electronic commerce transactions”, *Logistics Information Management*, Volume 15, Number 5/6, 2002, pp. 358-368.

[3] Chin, W.W. "The partial least squares approach to structural equation modeling," In Modern Methods for Business Research, Marcoulides, G.A. (ed.), Lawrence Erlbaum Associates, Mahwah, NJ, 1998, pp. I295–1336.

[4] Chin W., Newsted, P., “*Structural Equation Modeling Analysis with Small Samples Using Partial Least Squares*”, in Rick Hoyle (Ed.), Statistical Strategies for Small Sample Research, Sage Publications, 1999, pp. 307-341.

[5] Connolly, R. and Bannister, F. “Consumer trust in internet shopping in Ireland: towards the development of a more effective trust measurement instrument”, *Journal of Information Technology*, Volume 22, 2007, pp. 102-118.

[6] Fornell, C. and Larcker, D.F. "Evaluating structural equation models with unobservable variables and measurement error”, *Journal of Marketing Research*, Volume 18, Number 1, pp. 1981, 39-50.

[7] Goodhue, D., Lewis, W. and Thompson, R. "PLS, small sample size, and statistical power in MIS research*," Proceedings of the 39th Hawaii International Conference on System Sciences (HICSS 06),* Kauai, Hawaii, 2006.

[8] Ha, S. and Stoel, L. “Consumer e-shopping acceptance: antecedents in a technology acceptance model”, *Journal of Business Research*, Volume 62, Number 5, 2009, pp. 565–571.

[9] Halaweh, M. “Adoption of E-commerce: Understanding the Security Challenge”. *Electronic Journal of Information Systems in Developing Countries (EJISDC)*, Volume 47, Number (3), 2011, pp. 1-13.

[10] Haenlein, M., and Kaplan, A. “A beginner's guide to partial least squares analysis, Understanding Statistics”. *Statistical Issues in Psychology and Social Sciences*, Volume 3, Number 4, 2004, pp. 283-297.

[11] Hair, J.F., Black, W., C., Babin, B., J., Anderson, R., E., Tatham, R., L., “*Multivariate Data Analysis*”, 6th Edition, Pearson Prentice Hall, 2006.

[12] Khasawneh, A., Al Azzam, I. and Bsoul, M. “A study on e-commerce security in Jordan” *International Journal of Electronic Finance*, Volume 3, Number 2, 2009, pp. 166-176.

[13] Kim, C., Tao, W., Shin, N. and Kim, K. “An empirical study of customers’ perceptions of security and trust in e-payment systems”, *Electronic Commerce Research and Applications*, Volume 9, Number 1, 2010, pp. 84–95.

[14] Lallmahamood, M. “An Examination of Individual’s Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce: Using An Extension of the Technology Acceptance Model”, *Journal of Internet Banking and Commerce*, Volume 12, Number 3, 2007.

[15] Martinez-Ruiz, A. and Aluja-Banet, T. “Toward the Definition of a Structural Equation Model of Patent Value: PLS Path Modelling with Formative Constructs”, *Revstat – Statistical Journal*, Volume 7, Number 3, 2009, pp. 265–290.

[16] Salisbury, W., Pearson, R., Pearson, A., Miller, D. “Perceived security and World Wide Web purchase intention”, *Industrial Management & Data Systems*, Volume 101, Number 4, 2001, pp. 165-176.

[17] Sharma, A., and Yurcik, W. “A Study of E-Filing Tax Websites Contrasting Security Techniques Versus Security Perception”, *Proceedings of the*

Tenth Americas Conference on Information Systems, New York, USA, 5-8 August 2004.

[18] Singh, S. “The social dimensions of the security of internet banking”, *Journal of Theoretical and Applied Electronic Commerce Research*, Volume 1, Number 2, 2006, pp. 72 -78.

[19] Suh, B. 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, 2003, pp. 135-161.

[20] Ringle, C.M., S. Wende, and A. Will, SmartPLS 2.0 (beta). 2005, University of Hamburg: Hamburg, Germany.

[21] Teltzrow, M., Meyer, B. and Lenz, H. “Multichannel consumer perceptions”, *Journal of Electronic Commerce Research*, Volume 8, Number 1, 2007, pp.18-31.

[22] Turner, C., Zavod, M. and Yurcik, W. “Factors that Affect the Perception of Security and Privacy of E-Commerce Web Sites”, *Proceedings of the Fourth International Conference on Electronic Commerce Research*, Dallas, 2001, pp. 628-636.

[23] Turner, C. W. “The Online Experience and Consumers' Perceptions of E-Commerce Security” *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Volume 46, Number 14, September 2002, pp. 1246-1250.

[24] Urbach, N. and Ahlemann, F. “Structural equation modeling in information systems research Using partial least squares,” *Journal of Information Technology Theory and Application (JITTA)*, 2010, Volume 11, Number 2, pp. 5–40.

[25] Yenisey, M., Ozok, A. and Salvendy, G. “Perceived security determinants in e-commerce among Turkish university students”, *Behaviour and Information Technology*, Volume 24, Number 4, 2005, pp. 259-274.

[26] http://www.kikscore.com/misc/kikscoresurvey.pdf [Accessed 28th December 2011)

AUTHOR BIOGRAPHY

Mohanad Halaweh is an Assistant Professor in the College of Information Technology at University of Dubai (UD). He obtained his Ph.D. in Information Systems from De Montfort University, UK. His research appeared in journals such as Journal of Information Technology Theory and Application (JITTA), International Journal of Business Information Systems, Journal of Technology Management and Innovation, Electronic Journal of Information Systems in Developing Countries (EJISDC) and International Journal of E-Business Research. He has also published and participated in many international conferences in IS such as ICIS; a top-tier conference in IS field. His research focus is on E-commerce, Security and Privacy issues in E-commerce, IT Acceptance and Adoption, and IS Research Methods (mainly grounded theory).