Analysis of Perceived Security in B2C Electronic Commerce Website

Qin Yang

School of Business, Sichuan Agricultural University, Dujiangyan 611830, Sichuan, China

Yanwu Wang

School of Management, Huazhong University of Science and Technology, Wuhan 430074, China

Abstract

Customer loyalty or repeat purchasing is critical for the survival and success of any store. By focusing on online stores, this study investigates the repeat purchase intention of experienced online buyers based on means-end chain theory and prospect theory. Buyer concern about website security is a critical issue when it comes to maximizing the potential for electronic commerce transactions. Because perceptions of inadequacy can be a major obstacle to online shopping, many researchers have studied both the antecedents and outcomes of website security. Yet, the measures of security used in these studies are problematic. Although information systems researchers and business practitioners have conceptualized security as a multidimensional concept, published empirical studies have measured perceived security as a unidimensional construct. Exclusion of the underlying dimensions likely prevents researchers fromfully assessing the impact of important dimensions of customers' perceptions of security. Here, we contribute to the methodological enhancement of this research stream by: (1) theoretically examining the nature and dimensionality of perceived security, and (2) developing and validating a multidimensional measure of this construct. The results from this study provide empirical justification for the conceptualization of perceived security as a formative second-order construct of perceived confidentiality, perceived availability, and perceived nonrepudiation.

Key words: PERCEIVED SECURITY, PERCEIVED RISK, PROSPECT THEORY, TECHNOLOGY ACCEPTANCE MODEL (TAM), FORMATIVE CONSTRUCT

1. Introduction

As online retailing has grown rapidly worldwide and become globally competitive over the past decade, how to retain existing customers to make repeated purchases (hereafter referred to as repurchase) becomes a more important concern for online vendors than ever before (Johnson et al. 2008). In this context, a large number of studies have been conducted to understand what makes online customers repurchase from an online vendor. Among the many influencing factors, trust has been found to be a key predictor for customer retention (e.g., Flavian et al. 2006; Gefen 2002; Qureshi et al. 2009) due to its crucial ability to promote risk-taking behavior in the case of uncertainty, interdependence, and fear of opportunism (Mayer et al. 1995; McKnight et al. 1998).

The study reported here enhances the methodological rigor of IS research by: (1) theoretically examining the nature and dimensionality of perceived security, and (2) developing a reliable and valid multidimensional measure of perceived security. The more comprehensive and robust measure of perceived security allows more comprehensive testing of hypotheses related to the role of perceived security in online shopping and its impact on other endogenous variables.

We begin with a background about perceived security within the context of B2C e-commerce.We then identify and describe themost significant dimensions of perceived security, which are used to develop and test perceived security as a second-order construct with firstorder formative dimensions, which are themselves measured by reflective indicators [24]. We conclude by discussing implications of our findings for researchers and business practitioners, aswell as limitations of this study.

2. Background

Much of the research related to perceived security is rooted in the technology acceptance model (TAM) which is an information systems theory that predicts how users respond to new technology Their study develops a scale to measure perceived web security and applies that scale to investigate its impact on intent to purchase products using the B2C e-commerce sites. Moreover, they also investigate the impacts of two technology acceptance model's (TAM's) constructs, namely the perceived ease of use and perceived usefulnesswith respect to online shopping, on intent to purchase products using the B2C e-commerce sites. The statistical results show that higher level of perceived Web security leads to greater intent to purchase products using the B2C e-commerce sites. Additionally, impact of perceivedWeb security on purchase intention is stronger than those of perceived ease of use and of perceived usefulness with respect to online shopping.

Using TAM with an added construct of perceived Web security, Cheng, Lam, and Yeung [19] also demonstrate that perceivedWeb security, together with perceived usefulness and perceived ease of use, is significantly correlated with intention to use online banking sites.Chang and Chen [17] demonstrate that perceived security, together with interface quality, is a significant predictor of customer satisfaction on B2C e-commerce websites. The study also shows that these two factors significantly influence switching cost, which means that online customers tend to continue to use websites that they perceive as having high security and good interface quality.

Later studies of the role of perceived security in B2C e-commerce have linked perceived security to perceived trust and perceived risk (e.g., [10]). Cheung and Lee [20] investigate the impact of perceived security on trust in the B2C e-commerce context. Their study shows that perceived security, together with other factors, has considerable impact on consumer trust in online shopping.

Extending this research stream of perceived security within the B2C e-commerce context, our study theoretically examines the nature and dimensionality of perceived security, and creates a more robust, multidimensional measure of perceived security.

3. Measurement development

To ensure the quality of a measure, researchers must consider whether the indicators used in the measurement model should be modeled as reflective latent variables or as formative composite variables. This issue is important because it has implications for construct misspecification, construct identification, and construct validation [27].

Alternatively, the non-correlated indicators in a formative model influence the composite construct. Hence, the indicators actually cause the composite construct, and the construct is fully derived by the indicators [26]. Because each indicator is independent of the others, eliminating any one of the multiple indicators would change the conceptual meaning of the composite construct [13].

As discussed in more detail in the next section, dimensions of perceived security are distinct constructs that fully define the composite construct perceived security, not simply reflections or manifestations of the perceived security. Therefore, we model perceived security as a formative multidimensional construct [24].

For the specific measurement model used in this

study, we use the guideline for developing formative indexes suggested by Diamantopoulos and Winklhofer [25]. The first step is domain specification. In this step, literature is reviewed as a basis for specifying the conceptual domain of the perceived security construct, including its definition and relevant dimensions. The second step, indicator specification, involves a literature-based analysis designed to either identify or create the reflective indicators for each dimension of perceived security. The third step is indicator validation. In this step, the reflective indicators are validated as reliable and valid measures of the dimensions. By assessing both external validity and multicollinearity, the fourth step involves validation of perceived security as a formative second-order construct, with the relevant dimensions as the reflective first-order factors. Finally, a guideline is furnished for incorporating the second-order construct measure of perceived security into traditional statistical analyses.

3.1. Step 1: domain specification

This step involves specifying the construct domain of perceived security by developing the theoretical definition and identifying the conceptual dimensions of this construct. Our definition of perceived security reflects a comprehensive review of extant definitions in the IS, and other relevant, literature (e.g., computer science). The definition advanced here reflects the combined essence of perceived security definitions in these studies: The degree to which the online buyer believes that conducting an online transaction on the seller's website is safe in a manner consistent with the buyer's confident expectations.

The second part of the domain specification process involves the identification of relevant dimensions of perceived security. We review literature that examines issues in security, which includes not only perceived security but also objective security. The findings reveal that confidentiality, integrity, and availability are the earliest andmostwidely used dimensions. Recent studies have added non-repudiation, authentication, access control, communication security, and privacy to the original triad.

We evaluate all of these dimensions using relevance, non-redundancy, and completeness as criteria for inclusion. Relevance refers to the dimension being consistent with the definition and characterizes the essence of perceived security. Non-redundancy refers to the fact that the dimension should not overlap with another dimension. Completeness ensures that all relevant and non-redundant dimensions have been included. Based on these criteria, we select confidentiality, integrity, availability, and non-repudiation as focal dimensions of perceived security.

3.1.1. Confidentiality

Confidentiality refers to the degree to which improper disclosures of information are anticipated and prevented. Systems with superior confidentiality are better able to anticipate and prevent improper disclosure of information, such as leakage of information to an unauthorized party. A system's inability to anticipate and prevent improper disclosure of information may well indicate system insecurity. Common security measures to maintain confidentiality include encryption and authentication such as password-based and token-based authentication.

3.1.2. Integrity

Integrity refers to the degree to which improper modifications to information are anticipated and prevented. Systems with superior integrity are better able to anticipate and prevent improper modification of information, such as faulty alteration, deletion, or addition. While some erroneous modifications of information are accidental, others may be made intentionally by unauthorized parties. Common security measures to maintain integrity include digital signatures and anti-virus programs that prevent a virus from destroying data.

3.1.3. Availability

Availability refers to the degree to which information is available to authorized subjects when required. Systems with superior availability are better able to consistently provide relevant information to authorized parties. Common security measures to maintain availability include back-up systems and countermeasures for distributed-denialof- service attacks.

3.1.4. Non-repudiation

Non-repudiation in a buyer–seller exchange refers to the degree to which the systems is capable of ensuring that information sent by the customer is received by the person the seller claims to be. The goal is to ensure that the seller cannot later deny a completed transaction. Systems with superior non-repudiation are better able to provide verifiable proof of identity. Digital signature is a common security measure used to ensure non-repudiation.

Dimensions dropped due to their inconsistency with our definition of perceived security are authentication, access control, and communication security. These variables more appropriately represent countermeasures to protect information assets from security attacks. Privacy is also excluded because researchers tend to conceptualize privacy as being distinct from perceived security (e.g., [25]).

Table 1. Definitions of constructs.

Constructs		Definitions
Perceived confidentiality	PC	Online buyer's belief that his/her transactional information will not be disclosed to unauthorized party
Perceived integrity	PI	Online buyer's belief that his/her transactional information will not be altered by unauthorized party
Perceived availability	PA	Online buyer's belief about the online seller's ability and willingness to make information available to authorized subjects when required
Perceived non-repudiation	PNR	Online buyer's belief that the online seller cannot afterward deny the transaction that has been performed

Table 2. Demographic profiles of the respondents.

Demographic	variables	Frequency	Percentage
Gender	Female	159	32.5
	Male	329	67.3
	missing	1	0.2
Age	b20	69	14.1
	b30	250	51.1
	b40	143	29.3
	b50	22	4.5
	N=50	3	0.6
	Missing	2	0.4
Marriage	Married	140	28.6
	Unmarried	347	71.0
	Missing	2	0.4
Occupation	Housewife	6	1.2
	Student	180	36.8
Office	worker	261	53.4
	Self-employed	5	1.0
	Government	4	0.8
	Professional	27	5.5
	Others	2	0.4
	Missing	4	0.8
Education	Below	high	school
	High school	9	1.8
	College	student	198
	College	graduate	or
	Missing	13	2.7

Based on the framework of four dimensions, we develop a measure of perceived security as a second-order construct with four first-order formative dimensions: perceived confidentiality, perceived integrity, perceived availability, and perceived non-repudiation. The specific definition for each dimension is presented in Table 1.

Operationalization of perceived security as a formative second-order construct, instead of a reflective one, is consistent with the four criteria suggested by Jarvis and colleagues. First, the dimensions define characteristics rather than manifestations of perceived security. The extent to which the online buyer believes that conducting a transaction through the online seller's website is safe (i.e., perceived security) is characterized by the extent to which the customer believes that his/her transactional information will be neither disclosed (i.e., breach of perceived confidentiality) nor altered by an unauthorized party (i.e., breach of perceived integrity), that the online seller is able and willing to make information available to authorized customer when required (i.e., perceived availability), and that the online seller is really the entity he/she/it claims to be andwill be unable to deny

the completed transaction (i.e., perceived non-repudiation).

Second, a change in any of the dimension will alter the level of perceived security, but alteration of security perception does not necessarily change the level of all dimensions. For instance, if an online transaction is disrupted because of system failure (i.e., diminution in perceived availability), the customer's perceived security will be negatively impacted (i.e., diminution in perceived security). Yet, a reduction in perceived security does not induce a reduction in perceived availability.

Third, each dimension represents a distinct concept. The dimension definitions presented in Table 1 represent four distinct constructs that independently impact perceived security.

Table 3. Rotated factormatrix from EFA using SPSS principal axis factoring with Varimax rotation.

	Factor1	Factor2	Factor3
PA1	0.88		
PA2	0.86		
PA3	0.77		
PNR1		0.78	
PNR2		0.89	
PNR3		0.70	
PC1			0.84
PC2			0.93
PC3			0.91
PI2			0.60
PI3			0.77
PI1*	0.42	0.22	0.37

*: The indicator is eliminated.

Fourth, the dimensions are orthogonal and a change in one dimension does not induce changes in other dimensions. For example, the online buyer's disrupted transaction reduces the buyer's perceived systemavailability, but perceived confidentiality, integrity, and non-repudiation are not necessarily impacted. An empirical test of multicollinearity will allow us to test this assumption.

3.2. Step 2: indicator specification

Indicator specification involves a review of existing research to identify specific indicators required for measuring each of the dimensions. The conceptualization and measurement of perceived security have drawn considerable attention among scholars and practitioners in the IS discipline over the past decade. Much of the interest in this topic relates to the belief that lack of security for B2C e-commerce websites has been a major inhibitor to many consumers' willingness to engage in online shopping [25].

Previous empirical studies have used a variety of measures of perceived security. The analysis of these measures provides several useful indicators of the dimensions adopted for this study [20,18]. Because all dimensions do not appear in prior studies, we develop new indicators based on conceptual definitions of the dimensions as noted in Table 1. We model the indicators as reflective indicators of the dimensions on the basis of the following criteria as suggested by Jarvis et al.: (1) the indicators are manifestations of the dimension, (2) a change in the dimension is reflected by changes in all of its indicators, (3) all indicators share a common theme (which is the dimension that they measure) and, hence, dropping one indicator would not change the conceptual domain of its dimension, and (4) the indicators covary, and a change in the value of one indicator changes the values of other indicators.

Table 4. Construct reliability and convergent validity tests.

		Number of indicators	Range of loadings	Cronbach's alpha	Composite reliability	AVE
Perceived availability	PA	3	0.77–0.88	0.79	0.88	0.70
Perceived non-repudiation	PNR	3	0.64–0.90	0.72	0.83	0.62
Perceived confidentiality	PC	5	0.64–0.90	0.86	0.90	0.65

		Number of indicators	Range of loadings	Cronbach's alpha	Composite reliability	AVE
Perceived usefulness	USE	3	0.80–0.84	0.77	0.86	0.68
Perceived ease	of	use	EAS	4	0.61–0.87	0.56
Attitude ATT	4	0.70–0.87	0.83	0.88	0.67	0.67
Intention INT	4	0.78–0.88	0.87	0.91	0.72	0.72

Norms for convergent validity:
Range of loadings: N0.50: Good, N0.70: Excellent.
Cronbach's alphas: N0.70.
Composite reliability: N0.70.
AVE: N0.50.

3.3. Step 3: reflective measure validation

Consistent with the work of Anderson and Gerbing [2], we evaluate the reflective measurements of the dimensions for their content validity, construct reliability, convergent validity, and discriminant validity.

Content validity is established through an iterative process of reviewing and revising the indicator items by a group of potential respondents and experts. Initially, we created a list of potential indicators to measure the constructs. We then pretested these indicators with a group of 10 Korean online shopping mall customers and 3 online shoppingmall administrators. The reviewwas for itemclarity, relevance, and brevity. Reviewers' comments were used to revise the relevant items. This review process was repeated until all reviewers were satisfied and no further revisions were recommended.

In this study, each construct is measured via multiple indicators. The survey asks a respondent to rate the extent to which he or she agrees with the claim that is made in the indicator. All indicators are measured on a seven-point Likerttype scale. All of the scales are anchored at 1 as “strongly disagree” and 7 as “strongly agree”.

Convenience sampling was used to collect the data. This sampling method has been used by several published studies (e.g.). Three anonymous organizations, namely a large university, a private company, and a government office in Seoul, South Korea agreed to help collect data from their members. They allowed us to conduct an on-site survey and encouraged their members to participate. Members of these organizations were well educated; hence, we expected that many were experienced online shoppers that were knowledgeable about important aspects of online security. We visited these organizations and presented the survey questionnaires to 489 members who were willing and eligible to participate.

Each respondent was asked to identify a single online shopping mall with which he or she is familiar. The respondent was then asked to answer the questionnaire on the basis of his or her experience in using this online shopping mall. To encourage candid responses, all respondents were assured of confidentiality. These 489 respondents returned completed questionnaires. Responses from 53 respondents were excluded due to missing information. The result was 436 usable responses. Table 2 shows a demographic profile of the respondents.

Because data for both independent and dependent constructs were collected from the same source, we addressed the possibility of common method bias. We employed three techniques to assess and minimize common method variance [1]. First, some of the scales were reversed to ensure that all responses do not correspond to a larger effect. Second, the respondents were assured of the anonymity of their responses. Finally, we used the Harmon's one-factor test to check for the presence of common method bias. The results of principal component analysis for all indicator items, without rotation, show that these indicators do not form a single higher-order factor. This finding suggests that common method bias is not a serious cause for concern.

Table 5. Discriminant validity test.

	Perceived availability	Perceived non non-repudiation	Perceived confidentiality	Perceived usefulness	Perceived ease of use	Attitude	Intention
Perceived availability	0.84						
Perceived non-repudiation	0.06	0.79					

Perceived confidentiality	0.33	0.12	0.81				
Perceived usefulness	0.00	0.29	0.16	0.82			
Perceived ease of use	0.12	0.25	0.08	0.39	0.12		
Attitude	0.16	0.18	0.27	0.41	0.53	0.82	
Intention	0.08	0.14	0.29	0.43	0.47	0.70	0.85

The numbers in the diagonal are the square root of AVE.
The numbers in the lower left triangle are the correlation coefficients.

Following the test for common method bias, we use the data to validate the measures. In order to avoid merely fitting the measurement model into the data, following the procedures used in many published studies, we randomly split the data into two sets: a set of 136 responses and another set of 300 responses. The first set of data was used to conduct an exploratory factor analysis (EFA) using SPSS' principal axis factoring with Varimax rotation. This analysis was designed to determine the underlying factor structure of the 12 indicators used to measure the four dimensions of perceived security. The use of a sample of 136 cases for 12 indicators satisfies the recommended 10:1 ratio recommended by Nunnally , Arrindell and van der Ende [[3], p. 166], and Velicer and Fava.

The rotated factor matrix presented in Table 3 suggests that there are only three underlying factors. With the exception of itemPI1, all factor loadings are greater than 0.50. Item PI1 (“The site transmits my transactional information accurately”) is eliminated because it does not load strongly on any factor. The first factor includes the three indicators tomeasure perceived availability (PA1, PA2, PA3). The second factor includes the three indicators to measure perceived nonrepudiation (PNR1, PNR2, PNR3). Unexpectedly, the third factor includes five indicators. Three of the indicatorswere designed to measure perceived confidentiality (PC1, PC2, and PC3) and the two indicators (PI2 and PI3) were designed to measure perceived integrity. Hence, contrary to our initial expectation, results of the exploratory factor analysis reveal only three factors, namely perceived availability, perceived non-repudiation, and a factor that includes the indicators to measure perceived confidentiality and perceived integrity. This finding suggests that, while perceived confidentiality and perceived integrity may be conceptually distinct, they are not empirically different. A scree plot with only three eigenvalues greater than one provides additional evidence of a three-factor model.

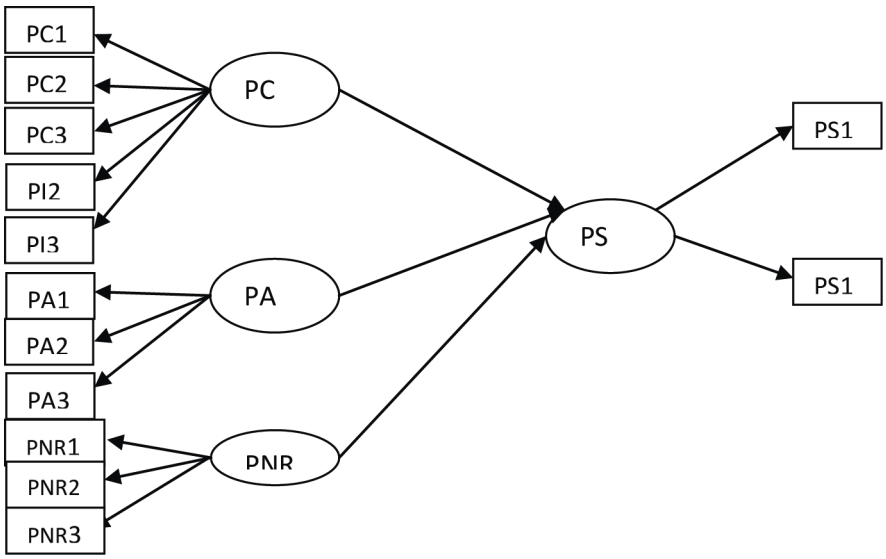

Figure 1. MIMIC model

While this result is unexpected, it is consistent with Schneider's andMotro's suggestions that these two dimensions are closely related, as confidentiality violations often occur concurrentlywith integrity violations. For instance, when an intruder intercepts a message stream of classified information, the intrud-

er must first read the information (i.e., confidentiality violation) before he or she can alter the information to meet specific objectives (i.e., integrity violation). After reanalyzing the operationalization of the two measures, their pairwise item correlations, and their distributions, we combine the two measures, with the result being labeled "perceived confidentiality." Generally speaking, this new confidentiality dimension measures or reflects a user's perception of the overall level of confidentiality provided by the online system.

Using the second set of 300 responses, we subjected the remaining indicators to AMOS' confirmatory factor analysis (CFA) by forcing each indicator to load according to the factor structure that is revealed in the exploratory analysis. The results suggest that the model fits the data well, as the various fit indices ($\chi 2$ = 98.16, d.f. = 41, GFI = 0.95, RMSEA = 0.07, NFI = 0.93, IFI = 0.96, CFI = 0.96) exceed established norms (i.e., GFI, NFI, IFI, CFI N .90 [8,12] and RMSEA b .08). Moreover, all path coefficients are statistically significant at p b 0.01

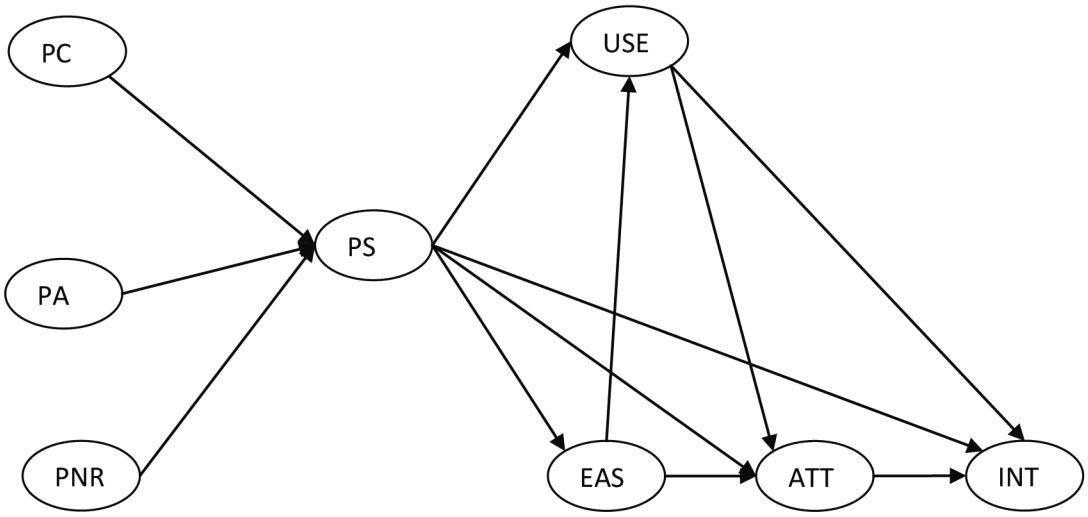

Figure 2. Structural model to test the nomological validity

Next,we analyzed the psychometric properties of each dimension to assess its construct reliability, convergent validity, and discriminant validity. Construct reliability is the assessment of internal consistency of the indicators of an individual construct. To assess the construct reliability, we computed both the Cronbach's alpha [22] and the composite reliability [30]. All Cronbach's alphas and the composite reliabilities exceed the benchmark of 0.70 (see Table 4) recommended by Nunnally and Bagozzi and Yi [6].

Convergent validity is evidenced when multiple attempts to measure the same construct generate similar results [5]. To assess the convergent validity, we computed the average variance extracted (AVE) for each construct. All AVEs (see Table 4) exceed the norm of 0.50, signifying convergent validity of the measure [30]. Moreover, results of the CFA show that every indicator loads significantly (p b 0.01) on the expected construct and that all loadings are above 0.60 (see Table 4), adding further evidence of the measure's convergent validity.

Discriminant validity refers to the extent to which measures of different concepts are distinct. To evaluate the discriminant validity, we compared the square root of average variance extracted (AVE) with the correlation coefficients between any two constructs. Table 5 shows that the AVE for each construct exceeds the square of the correlations between that construct and any other construct, thereby indicating adequate discriminant validity [30]. Taken together, these analyses demonstrate a high level of construct validity.

3.4. Step 4: formative second-order construct validation

Following indicator validation tests, we validated perceived security as a second-order construct with first-order formative dimensions. The initial part of this validation process tested for possible multicollinearity among the four dimensions. Multicollinearity is problematic for formative second-order constructs due to the underlying assumptions that the first-order factors are distinct aspects of the second-order construct. To test for possible multicollinearity, we computed bivariate correlations between any two dimensions and the variance inflation factor (VIF) for each dimension [7]. The results show that none of the correlations are greater than 0.33, which is far below the cutoff of 0.90, and that none of the VIFs are greater than 1.20, which is far below the cutoff of 3.0 [7].

The second step assessed external validity of

perceived security as a second-order construct with first-order formative dimensions. There are two recommended approaches for evaluating external validity: (1) the multiple indicators and multiple causes (MIMIC) model [25] and (2) the nomological validity test [4].

The MIMIC model presented in Fig. 1 includes the first-order constructs with both formative and reflective indicators [14]. This model shows how the formative second-order construct relates to two reflective indicators (PS1 and PS2) that capture the whole concept of the second-order construct — ("… global items that summarize the essence of the construct that the index claims to measure" [[25], p. 272]). Because no existing indicators were readily available, we also developed new indicators in this study. Results of the AMOS analysis show that all loadings are statistically significant (p b 0.01) and that the model yields a good fit ($\chi 2$ = 150.68, d.f. = 59, GFI = 0.93, RMSEA = 0.07, NFI = 0.90, IFI = 0.94, CFI = 0.94), suggesting acceptable external validity.

We further assess external validity by testing the nomological validity of perceived security as a second-order construct with first-order formative dimensions. We test whether or not the construct behaves as it should in a nomological network of relationships that are deduced from the technology acceptance model (TAM) [23].

First, we retest positive relationships of perceived security with user attitude (ATT) and intention (INT). Both perceived risk theory and prior studies support these relationships [23,19]. In the e-commerce environment, consumers tend to experience prepurchase uncertainty as to the type and degree of potential loss that might result from security breaches [15]. Hence, consumers who perceive that a website has a low level of security will also perceive a higher level of risk. The result is a negative attitude toward using this website. This negative attitude would be associated with a lower intention to use this website.

Second, we retest the relationship between perceived security and perceived usefulness (USE). While we found no study that directly tests the relationship between perceived security and perceived usefulness, a positive relationship is plausible. For instance, Gefen, Karahanna, and Straub [26] suggest that the usefulness of an e-commerce application is comprised of both short-term and long-term usefulness. An example of long-term usefulness is a site's ability to prevent a customer from incurring additional costs due to security breaches (e.g., unauthorized access and use of his/her credit card). Onewould expect that an increase in an e-commerce website's perceived security would increase the customer's belief that using this website would allow him/her to gain this long term benefit.

Finally, we retest the relationship between perceived security and perceived ease of use (EAS). Our decision to use only variables from the original TAM framework is rooted in our desire to keep the survey short to enhance response rate and the recognition that the relationships among the perceived security and various other TAM constructs have been well established.

SmartPLSwas used to analyze the structuralmodel of these relationships (Fig. 2). The results show that the model explains a nontrivial portion of the variance in perceived usefulness (R2 = 0.13), attitude (R2 = 0.26), intention (R2 = 0.41), and perceived ease of use (R2 = 0.03). The totality of these tests supports the external validity of the conceptualization of the perceived security as a second-order construct.

3.5. Step 5: operationalizing perceived security as a second-order construct in hypothesis testing

Our findings reveal a more complex factor structure for perceived security than those used in prior empirical studies. The indicators for perceived security arise from the first-order dimensions: perceived confidentiality, perceived availability, and perceived non-repudiation. For the perceived security measure, each indicator of the three dimensions (i.e., first-order factors) would be weighted by its factor score regression coefficient:

Perceived security= w_1PC1+ w_2PC2+ w_3PC3+ w_4PI2 + w_5PI3
+ w_6PA1 + w_7PA2 + w_8PA3+ w_9PNR1
+ w_{10}PNR2+ w_{11}PNR3.

This technique generates a more accurate measure as it reflects the influence of each item on the second-order factor.

4. Conclusions and implications

This study makes two important contributions to IS research. First, we both identify and validate three important dimensions of perceived security. Compared to prior studies that use measures of perceived security that tend to capture only one dimension or are dominated by only one dimension, the inclusion of these dimensions in themeasure of perceived security is more consistent with the way this construct has been conceptualized in earlier studies. Yet, knowledge that perceived confidentiality, perceived availability, and perceived non-repudiation are valid dimensions of perceived security should reveal a more detailed understanding of howeach component of perceived security impacts buyer intentions. Recognition of the major dimensions of perceived security provides re-

searchers an opportunity to add depth to their analyses and highlight the significance of each of these dimensions for improving customers' intentions.

Second, this study contributes to IS research methodology by developing and validating a robust formative second-order construct model of perceived security. The demonstrated reliability and validity of this multidimensionalmeasure should eliminate the use of the traditionally lower-quality, unidimensional measures of perceived security that have been popular in previous studies.Moreover, we provide a process for incorporating our second-order measure into standard statistical analysis techniques.

For IS practitioners, the results of this study suggest that perceived confidentiality, perceived availability, and perceived non-repudiation are important facets of perceived security, and that they play an important role in customers' decision to use a B2C e-commerce website. Collectively, they have significant impact on customers' perceived usefulness, ease of use, attitude, and intention to use B2C websites. Compared to prior studies, which use measures of perceived security that tend to capture only one dimension or are dominated by only one dimension, the inclusion of these dimensions in the measure of perceived security provides e-commerce website managers with a more comprehensive metric of perceived security. Such metric allows them to develop a richer understanding of how perceived security impacts their customers' willingness to use their websites for online purchases. Such understanding will help thempinpointwhere problems with perceived security might exist and, subsequently, make strategic decisions to enhance customers' perceived security.

The interpretation of our results is subject to some limitations. First, our empirical results must be considered in the context of the particular subjects included in the study. Second, the use of cross-sectional data allows us to examine only a “snapshot” of the impact of various antecedents on e-commercewebsite actual usage. Third, the use of convenience sampling may have the downside of diminishing the generalizability of the results. Building on the advances in this paper, future studies can consider the use of longitudinal datawhichwould reveal dynamics of this phenomenon over an extended period of time.

References

1. K.Amoako-Gyampah, J.R.Meredith (2007) Examining cumulative capabilities in a developing economy, *International Journal of Operations & Production Management* 27, p.p.928–950.
2. R.P. Bagozziv(1994) Measurement in marketing research: basic principles of questionnaire design, in: R.P. Bagozzi (Ed.). *Principles of Marketing Research*, Basil Blackwell Ltd., Massachusetts, USA.
3. A. Benlian, M. Koufaris, T. Hess (2011) Service quality in software-as-a-service: developing the SaaS-Qualmeasure and examining its role in usage continuance. *Journal of Management Information Systems*, 28(3), p.p.85-126.
4. P. Berghmans, K. Van Roy (2011) Information security risks in enabling e-government:the impact of IT vendors. *Information Systems Management*, 28(4), p.p.284-293.
5. A. Bhatnagar, S.Misra, H.R. Rao (2000) On risk, convenience, and Internet shopping behavior. *Communications of the ACM*, 43(11), p.p.98-105.
6. L.D. Bodin, L.A. Gordon, M.P. Loeb (2005) Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM*, 48(2) p.p.79-83.
7. K.A. Bollen (1989) Structural Equations with Latent Variables, John Wiley & Sons, New York.
8. M. Bruhn, D. Georgi, K. Hadwich (2008) Customer equity management as formative second-order construct, *Journal of Business Research*, 61(12) , p.p.1292-1301.
9. L. Casaló, C. Flavián, M. Guinalíu (2007) The role of security privacy, usability and reputation in the development of the online banking. *Online Information Review*, 31(5) p.p.583-603.
10. C. Cegielski (2008) Toward an interdisciplinary information assurance curriculum: knowledge and skill sets required of information assurance professionals. *Decision Sciences Journal of Innovative Education*, 6(1), p.p.29-49.
11. H.H. Chang, S.W. Chen (2009) Consumer perception of interface quality, security, and loyalty in electronic commerce. *Information & Management*, 46 (7), p.p.411-417.
12. R.K. Chellappa, P.A. Pavlou (2002) Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*,15(5), p.p.358-368.
13. T.C.E. Cheng, D.Y.C. Lam, A.C.L. Yeung (2006) Adoption of Internet banking: an empirical study in Hong Kong. *Decision Support Systems,* 42, p.p.1558-1572.
14. C.M.K. Cheung, M.K.O. Lee (2001) Trust in

Internet shopping: instrument development and validation through classical and modern approaches. *Journal of Global Information Management*, 9(3), p.p.23-35.
15. C.M.K. Cheung, M.K.O. Lee (2006) Understanding consumer trust in Internet shopping: a multidisciplinary approach. *Journal of the American Society for Information Science and Technology*, 57, p.p.479-492.
16. A. Diamantopoulos, P. Riefler, K.P. Roth (2008) Advancing formative measurement models. *Journal of Business Research*, 6, p.p.1203-1218.
17. A. Diamantopoulos, H. Winklhofer (2001) Index construction with formative indicators: an alternative to scale development. *Journal of Marketing Research*, 37, p.p.269-277.
18. T.E. Dube, R.A. Raines, G.L. Peterson, K. Bauer, M.R. Grimaila, S.K. Rogers (2012) Malware target recognition via static heuristics. *Journal of Computer Security*, 31, p.p.137-147.
19. Z. Erlich, M. Zviran (2010) Goals and practices in maintaining information systems security. *International Journal of Information Security and Privacy*, 4(3), p.p.40-50.
20. X. Fang, S. Chan, J. Brzezinski, S. Xu (2006) Moderating effects of task type onwireless technology acceptance, *Journal of Management Information Systems*, 22 p.p.123-157.
21. C. Flavian, M. Guinaliu (2006) Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site, *Industrial Management & Data Systems*,106, p.p.601-620.
22. R. Freeze, R.L. Rachke (2007) An assessment of formative and reflective constructs in IS research. *ECIS Proceedings*, p.p.171.
23. D. Gefen (2000) E-commerce-the role of familiarity and trust. *OMEGA*, 28(6), p.p.725-737.
24. D. Gefen, E. Karahanna, D.W. Straub (2003) Trust and TAMin online shopping: an integrated model. *MIS Quarterly*, 27, p.p.51-90.
25. L.A. Gordon, M.P. Loeb, L. Zhou (2011) The impact of information security breaches: has there been a downward shift in costs? *Journal of Computer Security*, 19(1), p.p.33–56.
26. V.K. Gurbani, A. McGee (2007) An early application of the Bell Labs Security framework to analyze vulnerabilities in the Internet telephony domain. *Bell Labs Technical Journal*, 12 (3), p.p.7-19.
27. J.F. Hair Jr., W.C. Black, B.J. Babin, R.E. Anderson, R.L. Tatham (2006) *Multivariate Data Analysis,* 6th ed., Prentice Hall, Upper Saddle.
28. Olbrich, R., and Holsing, C. (2011) Modeling consumer purchasing behavior in social shopping communities with clickstream data. *International Journal of Electronic Commerce,* 16(2), p.p.15-40.
29. Pagani, M., and Mirabello (2011) A. The influences of personal and social-interactive engagements in social TV Web sites. *International Journal of Electronic Commerce,* 16(2), p.p.41-67.
30. Turban, E., Bolloju, N., and Liang, T.P. (2011) Enterprise social networks. *Journal of Organizational Computing and Electronic Commerce,* 21(3), p.p.202-220.
31. Turban, E., Liang, T.P., and Wu, S. (2011) A framework for adopting collaboration 2.0 tools for virtual group decision making. *Group Decisions and Negotiation,* 20(2), p.p.137-154.
32. Zwass, V.(2010) Co-creation: Toward a taxonomy and an integrated research perspective. *International Journal of Electronic Commerce,* 15(1), p.p.11-48.