Decision Support Systems 62 (2014) 11–21

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Measuring perceived security in B2C electronic commerce website usage: A respecification and validation

Edward Hartono [a,1], Clyde W. Holsapple [b,2], Ki-Yoon Kim [c], Kwan-Sik Na [d,*], James T. Simpson [e,3]

[a] *Department of Accounting & MIS, Alfred Lerner College of Business & Economics, University of Delaware, Newark, DE 19716, United States*
[b] *Gatton College of Business & Economics, University of Kentucky, Lexington, KY 40506, United States*
[c] *School of Business, Kwangwoon University, 26 Kwangwoon-gil, Wolgye-dong, Nowon-gu, Seoul 139-701, Republic of Korea*
[d] *Department of Management Information Systems, Seowon University, 241 Musimseoro, Hungduk-gu, Cheongju-shi, Chungbuk 361-742, Republic of Korea*
[e] *Department of Management, Marketing, and Information Systems, College of Business Administration, University of Alabama in Huntsville, 301 Sparkman Drive, Huntsville, AL 35899, United States*

ARTICLE INFO

Article history:
Received 15 August 2013
Received in revised form 15 January 2014
Accepted 21 February 2014
Available online 10 March 2014

Keywords:
Perceived security
Electronic commerce
Online shopping
Technology acceptance model (TAM)
Second-order construct
Formative construct

ABSTRACT

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 from fully 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 non-repudiation.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

Internet technology and the variety of the resulting applications have revolutionized the way customers do business and interact with sellers of commercial products and services. In the retail industry, websites for business-to-consumer electronic commerce (B2C e-commerce) provide more accessible, easier, faster, and cheaper methods for individual consumers to conduct their retail transactions. As a result, online shopping has continued to gain popularity as a transaction medium.

The growing popularity of online shopping has been accompanied by rising concerns about Internet security. In fact, consumer surveys reveal that concerns with security are the consumers' top reason for avoiding online shopping [39,37,58]. *Perceived security* has become an important variable in B2C e-commerce consumers' decision-making model. Consequently, the future of B2C e-commerce may well depend on the selling firm's ability to manage security threats and improve consumer perceptions of Internet security [28]. This premise has resulted in perceived security becoming a major discussion and research topic among information systems (IS) professionals and academics.

An extensive review of perceived security literature reveals an inconsistency between the conceptualization of security and the operationalization of the measures of perceived security in empirical studies. The literature suggests that IS practitioners and researchers generally agree that security is a multidimensional construct that is derived from several underlying dimensions (e.g., confidentiality, integrity, availability, non-repudiation). Yet, most empirical studies ignore the multidimensionality of perceived security and use measures that tend to capture only one dimension or are dominated by only one dimension of perceived security. While these studies add to an understanding of the role of perceived security in a variety of exchange environments, exclusion of the underlying dimensions prevents us from recognizing their significance, and therefore, such analyses may lack important details.

* Corresponding author.
E-mail addresses: hartono@udel.edu (E. Hartono), cwhols@uky.edu (C.W. Holsapple), min1203@kw.ac.kr (K.-Y. Kim), ksna@seowon.ac.kr (K.-S. Na), simpsonj@uah.edu (J.T. Simpson).
[1] Tel.: +1 302 831 6144.
[2] Tel.: +1 859 257 5236.
[3] Tel.: +1 256 824 6408.

http://dx.doi.org/10.1016/j.dss.2014.02.006
0167-9236/© 2014 Elsevier B.V. All rights reserved.

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 the most significant dimensions of perceived security, which are used to develop and test perceived security as a second-order construct with first-order formative dimensions, which are themselves measured by reflective indicators [24]. We conclude by discussing implications of our findings for researchers and business practitioners, as well 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 [66]. The premise is that external variables such as perceived security influence how and when users will use new technology. To the best of our knowledge, studies that investigate the role of perceived security in the B2C context began with the publication of the empirical study by Salisbury, Pearson, Pearson, and Miller [66]. 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 usefulness with 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 perceived Web 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 perceived Web security, together with perceived usefulness and perceived ease of use, is significantly correlated with intention to use online banking sites. Lian and Lin [47] show that perceived security, together with personal innovativeness, personal privacy concern, personal product involvement, products and service types, is an important determinant of attitude toward online shopping. 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 (e.g., [32,33]) 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. Flavian and Guinaliu [29] confirm this result by demonstrating that increased customer perception of B2C e-commerce website security will result in greater trust and loyalty in the website. Adding perceived risk to the model, Kim, Ferrin, and Rao [45] investigate the impact of perceived security on both trust and perceived risk in the B2C context. The result of their study shows that perceived security, together with other factors, is an important antecedent of both trust and risk.

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 [31].

Reflective models include indicator variables that are influenced by the latent variables, where changes in the underlying latent construct are reflected by changes in the indicator variables. The indicator variables should be highly correlated, and the removal of an indicator should not alter the conceptual meaning of the latent construct [41].

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 [31]. 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). Appendix A includes a large sample of perceived security definitions proposed in various research studies. 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, which are reported in Appendix B, reveal that confidentiality, integrity, and availability are the earliest and most widely 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 [75]. 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 [75]. 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 [75]. 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-denial-of-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 [71]. 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., [29,64,81]).

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	<20	69	14.1
	<30	250	51.1
	<40	143	29.3
	<50	22	4.5
	>=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	1	0.2
	High school	9	1.8
	College student	198	40.5
	College graduate or over	268	54.8
	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 [41]. 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 and will 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 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 3
Rotated factor matrix from EFA using SPSS principal axis factoring with Varimax rotation.

	Factor 1	Factor 2	Factor 3
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 system availability, 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 [28,66].

Previous empirical studies have used a variety of measures of perceived security. Examples of these measures are detailed in Appendix C. The analysis of these measures provides several useful indicators of the dimensions adopted for this study [20,18,80,69]. 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. [41]: (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.

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 shopping mall administrators. The review was for item clarity, 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.

Appendix D shows the final list of indicators for measuring the dimensions of perceived security, plus additional constructs that were used to perform the external validity test. 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 Likert-type 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., [53,43,44]). 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 [61,1,42,62,68]. 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

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
Perceived usefulness	USE	3	0.80–0.84	0.77	0.86	0.68
Perceived ease of use	EAS	4	0.61–0.87	0.77	0.83	0.56
Attitude	ATT	4	0.70–0.87	0.83	0.88	0.67
Intention	INT	4	0.78–0.88	0.87	0.91	0.72

Norms for convergent validity:
Range of loadings: >0.50: Good, >0.70: Excellent.
Cronbach's alphas: >0.70.
Composite reliability: >0.70.
AVE: >0.50.

Table 5
Discriminant validity test.

	Perceived availability	Perceived 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	**0.75**		
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.

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.

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 [74], 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 [[56], p. 276], Arrindell and van der Ende [[3], p. 166], and Velicer and Fava [[79], p. 232].

The rotated factor matrix presented in Table 3 suggests that there are only three underlying factors. With the exception of item PI1, 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 to measure perceived availability (PA1, PA2, PA3). The second factor includes the three indicators to measure perceived non-repudiation (PNR1, PNR2, PNR3). Unexpectedly, the third factor includes five indicators. Three of the indicators were 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.

While this result is unexpected, it is consistent with Schneider's [67] and Motro's [54] suggestions that these two dimensions are closely related, as confidentiality violations often occur concurrently with integrity violations. For instance, when an intruder intercepts a message stream of classified information, the intruder 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 > .90 [8,12] and RMSEA < .08 [40]). Moreover, all path coefficients are statistically significant at $p < 0.01$.

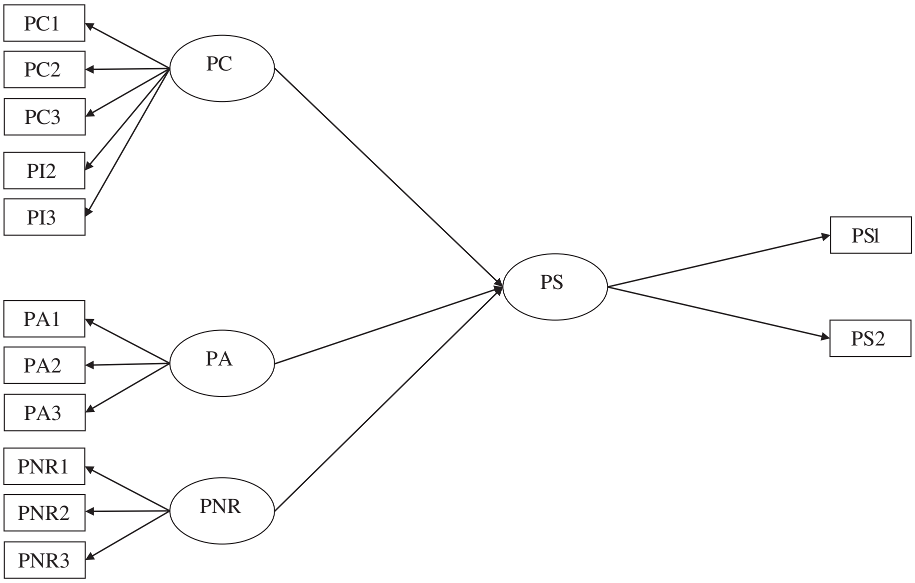

Fig. 1. MIMIC model.

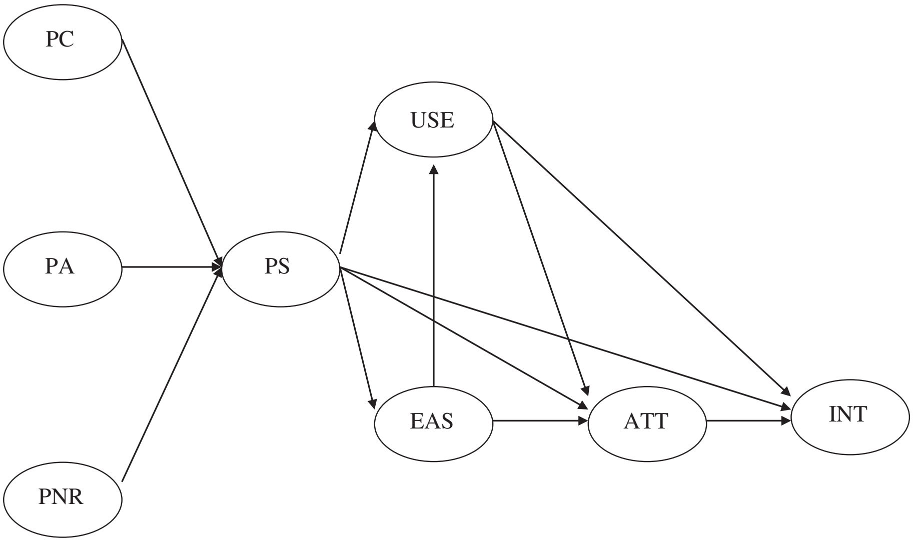

Fig. 2. Structural model to test the nomological validity.

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 [56] 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 [30,72]. Moreover, results of the CFA show that every indicator loads significantly ($p < 0.01$) on the expected construct and that all loadings are above 0.60 (see Table 4), adding further evidence of the measure's convergent validity [72].

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 [36].

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 [60,41]. 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]) (see Appendix D). 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 ($p < 0.01$) 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.

Table 6
Results of the structural model.

Paths	Coefficients	Standard error	t-Statistics
Perceived security → Perceived usefulness	0.13*	0.06	2.13
Perceived security → Perceived ease of use	0.18**	0.07	2.79
Perceived security → Attitude	0.16**	0.05	3.18
Perceived security → Intention	0.11*	0.04	2.57
Perceived ease of use → Perceived usefulness	0.31**	0.06	5.41
Perceived usefulness → Attitude	0.19**	0.05	3.97
Perceived usefulness → Intention	0.18**	0.05	3.97
Perceived ease of use → Attitude	0.35**	0.05	6.91
Attitude → Intention	0.51**	0.05	10.55

* Significant at 5% level of significance.
** Significant at 1% level of significance.

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 [66,49,28,19]. In the e-commerce environment, consumers tend to experience pre-purchase 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 [33] 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). One would 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). Previous studies [51] have shown a positive relationship between perceived security and perceived ease of use. Perceived ease of use includes the user's personal comfort with the systems [76]. High levels of perceived security should cause the user to feel more comfortable with using the system.

It should be noted that there are other constructs that have been added to the perceived security–TAM framework. Two of the most popular are trust and perceived risk (e.g., [45]). 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.

SmartPLS was used to analyze the structural model of these relationships (Fig. 2). The results show that the model explains a nontrivial portion of the variance in perceived usefulness ($R^2 = 0.13$), attitude ($R^2 = 0.26$), intention ($R^2 = 0.41$), and perceived ease of use ($R^2 = 0.03$). All factor loadings are statistically significant at a 5% level (see Table 6). 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*.

In hypothesis testing, measure for a second-order construct is usually the simple average of reflective indicators of the first-order dimensions [55,38]. Simpson and Paul [70] have proposed an improved technique, where each indicator of the first-order dimensions is weighted by the factor score regression coefficient. 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:

$$\begin{aligned}\text{Perceived security} = {} & w_1 PC1 + w_2 PC2 + w_3 PC3 + w_4 PI2 + w_5 PI3 \\ & + w_6 PA1 + w_7 PA2 + w_8 PA3 + w_9 PNR1 \\ & + w_{10} PNR2 + w_{11} PNR3.\end{aligned}$$

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 the measure of perceived security is more consistent with the way this construct has been conceptualized in earlier studies. Moreover, this inclusion should encourage more detailed analyses that include the impact of each dimension on other important variables in the model. For instance, previous studies have demonstrated that perceived security positively impacts customers' intention to use B2C e-commerce websites [66]. Yet, knowledge that perceived confidentiality, perceived availability, and perceived non-repudiation are valid dimensions of perceived security should reveal a more detailed understanding of how each component of perceived security impacts buyer intentions. Recognition of the major dimensions of perceived security provides researchers 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 multidimensional measure 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 them pinpoint where 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. The exclusive use of Korean respondents has the advantage of excluding unwanted confounding factors resulting from cultural differences. Yet, it also has the disadvantage of reducing the generalizability of the results. Second, the use of cross-sectional data allows us to examine only a "snapshot" of the impact of various antecedents on e-commerce website 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 data which would reveal dynamics of this phenomenon over an extended period of time.

Appendix A. Survey of perceived security definitions

Studies	Definitions of perceived security
Salisbury et al. [66] Cheng et al. [19] Liao and Wong [48]	The extent to which one believes that the Web is secure for transmitting sensitive information
Cheung and Lee [20] Cheung and Lee [21]	The perception of Internet shoppers of Internet merchants' ability to fulfill security requirements
Chellappa and Pavlou [18]	The subjective probability with which consumers believe that their personal information will not be viewed, stored or manipulated during transit or storage by inappropriate parties, in a manner consistent with their confident expectations
Liu et al. [50]	The perception that making a transaction with an Internet store is safe
Yenisey et al. [80]	The level of security that users feel while they are shopping on e-commerce sites
Fang et al. [28]	The extent to which a user believes that using a particular application will not expose his or her private information to any unauthorized party
Lian and Lin [47]	One's awareness of Web security when providing and sending personal or financial information
Flavian and Guinaliu [29]	The subjective probability with which consumers believe that their personal information (private and monetary) will not be viewed, stored, and manipulated during transit and storage by inappropriate parties in a manner consistent with their confident expectations
Chang and Chen [17]	Customer perceptions of the security of the transaction as a whole
Roca et al. [64]	The customers' perception of the degree of protection against a threat that creates a circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosures, modification of data, denial of service, and/or fraud, waste and abuse
Yousafzai et al. [81]	The customers' perception of the degree of protection against destruction, disclosure, modification of data, fraud, and abuse
Kim et al. [46]	The customer's subjective evaluation of the system's security

Appendix B. Survey of security dimensions

Studies	Dimensions of security
Bodin et al. [11] Ryan and Ryan [65] Erlich and Zviran [27] Berghmans and Van Roy [9] Gordon et al. [34] Dube et al. [26] Ransbotham et al. [63]	Confidentiality, integrity, availability
Siponen and Kukkonen [70]	Confidentiality, integrity, availability, non-repudiation
Cegielski [16] Vaidyanathan and Mautone [77] McFadzean et al. [52]	Confidentiality, integrity, availability, authentication, non-repudiation
Parent [59]	Confidentiality, integrity, availability, authentication, access control, non-repudiation
Gurbani and McGee [35]	Confidentiality, integrity, availability, authentication, access control, non-repudiation, communications security, privacy

Appendix C. Survey of the perceived security measures

Studies	Indicators of perceived information security
Salisbury et al. [66] Cheng et al. [19] Vatanasombut et al. [78] Chang and Chen [17]	1. I would feel secure sending sensitive information across the World Wide Web 2. The World Wide Web is a secure means through which to send sensitive information 3. I would feel totally safe providing sensitive information about myself over the World Wide Web 4. Overall, the World Wide Web is a safe place to transmit sensitive information
Cheung and Lee [20] Cheung and Lee [21]	1. Internet vendors implement security measures to protect Internet shoppers 2. Internet vendors have the ability to verify Internet shoppers' identity for security purposes 3. Internet vendors usually ensure that transactional information is protected from being accidentally altered or destroyed during transmission on the Internet
Chellappa and Pavlou [18]	1. The degree of confidence that information will only reach the appropriate party 2. The degree of confidence that inappropriate parties would neither view nor store consumer information 3. The degree of confidence that the retailer will not expose consumer information to others 4. The degree of confidence that inappropriate parties will not manipulate consumer information during transaction 5. The degree of overall confidence in the transaction's security
Liu et al. [50]	1. I believe that shopping on this Internet store is just as safe as placing an order by phone 2. It is just as safe to make a credit card purchase at this Internet store as it is to make one in person 3. The data transmission between my computer and this Internet store is safe 4. This Internet store is capable of preventing illegal access
O'Cass and Fenech [57] Lian and Lin [47]	1. I feel secure sending personal information across the Web 2. I feel safe providing personal information about me to Web retailer 3. Web is a safe environment to provide personal information
Yenisey et al. [80] Shin [69]	1. I believe the information I provide with SNS will not be manipulated by inappropriate parties 2. I am confident that the private information I provide with SNS will be secured. 3. I believe inappropriate parties may deliberately view the information I provide with this SNS
Fang et al. [28]	1. I feel secure to perform this task on the handheld computer 2. There is feedback indicating the information is protected
Flavian and Guinaliu [29]	1. I think this website has mechanisms to ensure the safe transmission of its users' information 2. I think this website shows great concern for the security of any transactions 3. I think this website has sufficient technical capacity to ensure that no other organization will supplant its identity on the Internet 4. I am sure of the identity of this website when I establish contact via the Internet

Appendix C *(continued)*

Studies	Indicators of perceived information security
	5. When I send data to this website, I am sure that they will not be intercepted by unauthorized third parties 6. I think this website has sufficient technical capacity to ensure that the data I send will not be intercepted by hackers 7. When I send data to this website, I am sure they cannot be modified by a third party 8. I think this website has sufficient technical capacity to ensure that the data I send cannot be modified by a third party
Liao and Wong [48]	1. The Internet e-banking systems restrict unauthorized access 2. The Internet e-banking systems protect customer private data 3. The Internet e-banking systems have rigorous security control
Roca et al. [64]	1. I think the online trading systems have sufficient technical capacity to ensure that the data I send cannot be modified by a third party 2. The online trading systems have enough security measures to protect my personal and financial information 3. When I send data to the online trading systems, I am sure that they will not be intercepted by unauthorized third parties 4. I think the online trading systems have sufficient technical capacity to ensure that no other organization will supplant its identity on the Internet
Yousafzai et al. [81]	1. I believe my Internet banking transaction information will not be lost during an online session 2. I believe my Internet banking transaction information will only reach the target bank account 3. While using Internet banking, I believe that the security system will confirm my identity before disclosing account information 4. While using Internet banking, I believe that the security system will confirm my identity before processing transactions 5. While using Internet banking, I believe that the security system does not allow unauthorized access to the account 6. While using Internet banking, I believe that the security system stops any unauthorized changes to a transaction 7. While using Internet banking, I believe that the security system provides a secure environment in which to bank
Shin [69]	1. In general, I feel secure in using IPTV system. 2. I feel safe in transaction, downloading contents (VoD), and accessing sites via IPTV. 3. IPTV is well built against security-related concerns such as hacking, unauthorized uses, theft of data, interception of transmission, and virus.
Kim et al. [46]	1. I perceive EPS as secure 2. I perceive the information relating to user and EPS transactions as secure 3. The information I provided in previous EPS is helpful for secure payment transactions 4. I do not fear hacker invasions into EPS
Swilley [73]	1. I feel secure putting credit card information on my cell phone 2. I feel secure putting personal information, such as my driver's license number on a wallet phone. 3. I feel safe in my transactions with a wallet phone 4. I feel like my privacy is protected on a wallet phone 5. I feel I can trust having my information on a wallet phone

Appendix D. Indicators of the constructs

All indicators are measured on a seven-point Likert-type scale (1: "strongly disagree" to 7: "strongly agree"). To each online consumer, we ask the extent to which he or she agrees with the following statements.

Constructs	Indicators
Perceived confidentiality	PC1. Someone uses my Internet ID to read my transactional information. [R] PC2. Someone uses my Internet ID to make order. [R] PC3. Someone steals my Internet ID. [R]
Perceived integrity	PI1. The site transmits my transactional information accurately. [D] PI2. My transactional information is altered. [R] PI3. The site records my transactional information incorrectly. [R]
Perceived availability	PA1. I cannot order due to system failure. [R] PA2. I cannot order due to database failure. [R] PA3. I cannot order due to network failure. [R]
Perceived non-repudiation	PNR1. This site uses digital signature PNR2. The legislation backs up the digital signature PNR3. The identity of this site is trustworthy
Perceived ease of use	EAS1. It is easy to place an order EAS2. It is easy to shop EAS3. It is easy to learn the shopping procedure EAS4. Everyone can easily master the shopping procedure
Perceived usefulness	USE1. This site is very informative USE2. I can easily find the product that I am looking for USE3. I can easily get the information that I need
Attitude	ATT1. It is a good idea to shop in this site ATT2. It is a smart idea to shop in this site ATT3. It is enjoyable to shop in this site ATT4. I feel positive to shop in this site
Intention	INT1. This site will be my first option whenever I want to shop INT2. I will use this site again INT3. I will use this site regularly INT4. I will use this site frequently
Perceived security (global indicators)	PS1. My personal information is securely managed in this site PS2. This site is safe for my personal information

[D] Indicator is eliminated.

[R] Reverse-scale indicator.

References

[1] K. Amoako-Gyampah, J.R. Meredith, Examining cumulative capabilities in a developing economy, International Journal of Operations & Production Management 27 (2007) 928–950.

[2] J.C. Anderson, D.W. Gerbing, Structural equation modeling in practice: a review and recommended two-step approach, Psychological Bulletin 103 (1988) 411–423.

[3] W.A. Arrindell, J. van der Ende, An empirical test of the utility of the observations-to-variables ratio in factor and components analysis, Applied Psychological Measurement 9 (1985) 165–178.

[4] R.P. Bagozzi, Measurement in marketing research: basic principles of questionnaire design, in: R.P. Bagozzi (Ed.), Principles of Marketing Research, Basil Blackwell Ltd., Massachusetts, USA, 1994.

[5] R.P. Bagozzi, Representing and testing organizational theories: a holistic construal, Administrative Science Quarterly 27 (3) (1982) 459–489.

[6] R.P. Bagozzi, Y. Yi, On the evaluation of structural equation models, Journal of the Academy of Marketing Science 16 (1988) 74–94.

[7] A. Benlian, M. Koufaris, T. Hess, Service quality in software-as-a-service: developing the SaaS-Qual measure and examining its role in usage continuance, Journal of Management Information Systems 28 (3) (2011) 85–126.

[8] P.M. Bentler, D.G. Bonnet, Significance tests and goodness of fit in the analysis of covariance structures, Psychological Bulletin 88 (1980) 588–606.

[9] P. Berghmans, K. Van Roy, Information security risks in enabling e-government: the impact of IT vendors, Information Systems Management 28 (4) (2011) 284–293.

[10] A. Bhatnagar, S. Misra, H.R. Rao, On risk, convenience, and Internet shopping behavior, Communications of the ACM 43 (11) (2000) 98–105.

[11] L.D. Bodin, L.A. Gordon, M.P. Loeb, Evaluating information security investments using the analytic hierarchy process, Communications of the ACM 48 (2) (2005) 79–83.

[12] K.A. Bollen, Structural Equations with Latent Variables, John Wiley & Sons, New York, 1989.

[13] K.A. Bollen, R. Lennox, Conventional wisdom on measurement — a structural equation perspective, Psychological Bulletin 110 (2) (1991) 305–314.

[14] M. Bruhn, D. Georgi, K. Hadwich, Customer equity management as formative second-order construct, Journal of Business Research 61 (12) (2008) 1292–1301.

[15] L. Casaló, C. Flavián, M. Guinalíu, The role of security privacy, usability and reputation in the development of the online banking, Online Information Review 31 (5) (2007) 583–603.

[16] C. Cegielski, Toward an interdisciplinary information assurance curriculum: knowledge and skill sets required of information assurance professionals, Decision Sciences Journal of Innovative Education 6 (1) (2008) 29–49.

[17] H.H. Chang, S.W. Chen, Consumer perception of interface quality, security, and loyalty in electronic commerce, Information & Management 46 (7) (2009) 411–417.

[18] R.K. Chellappa, P.A. Pavlou, Perceived information security, financial liability and consumer trust in electronic commerce transactions, Logistics Information Management 15 (5) (2002) 358–368.

[19] T.C.E. Cheng, D.Y.C. Lam, A.C.L. Yeung, Adoption of Internet banking: an empirical study in Hong Kong, Decision Support Systems 42 (2006) 1558–1572.

[20] C.M.K. Cheung, M.K.O. Lee, Trust in Internet shopping: instrument development and validation through classical and modern approaches, Journal of Global Information Management 9 (3) (2001) 23–35.

[21] C.M.K. Cheung, M.K.O. Lee, Understanding consumer trust in Internet shopping: a multidisciplinary approach, Journal of the American Society for Information Science and Technology 57 (2006) 479–492.

[22] L.J. Cronbach, Coefficient alpha and the internal structure of tests, Psychometrika 16 (1951) 297–334.

[23] F.D. Davis, R.P. Bagozzi, P.R. Warshaw, User acceptance of computer technology: a comparison of two theoretical models, Management Science 35 (1989) 982–1003.

[24] A. Diamantopoulos, P. Riefler, K.P. Roth, Advancing formative measurement models, Journal of Business Research 61 (2008) 1203–1218.

[25] A. Diamantopoulos, H. Winklhofer, Index construction with formative indicators: an alternative to scale development, Journal of Marketing Research 37 (2001) 269–277.

[26] T.E. Dube, R.A. Raines, G.L. Peterson, K. Bauer, M.R. Grimaila, S.K. Rogers, Malware target recognition via static heuristics, Journal of Computer Security 31 (2012) 137–147.

[27] Z. Erlich, M. Zviran, Goals and practices in maintaining information systems security, International Journal of Information Security and Privacy 4 (3) (2010) 40–50.

[28] X. Fang, S. Chan, J. Brzezinski, S. Xu, Moderating effects of task type on wireless technology acceptance, Journal of Management Information Systems 22 (2005–2006) 123–157.

[29] C. Flavian, M. Guinaliu, Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site, Industrial Management & Data Systems 106 (2006) 601–620.

[30] C. Fornell, D. Larcker, Evaluating structural equation models with unobservable variables and measurement error, Journal of Marketing Research 18 (1981) 39–50.

[31] R. Freeze, R.L. Rachke, An assessment of formative and reflective constructs in IS research, ECIS Proceedings, 2007, p. 171, (paper).

[32] D. Gefen, E-commerce — the role of familiarity and trust, OMEGA 28 (6) (2000) 725–737.

[33] D. Gefen, E. Karahanna, D.W. Straub, Trust and TAM in online shopping: an integrated model, MIS Quarterly 27 (2003) 51–90.

[34] L.A. Gordon, M.P. Loeb, L. Zhou, The impact of information security breaches: has there been a downward shift in costs? Journal of Computer Security 19 (1) (2011) 33–56.

[35] V.K. Gurbani, A. McGee, An early application of the Bell Labs Security framework to analyze vulnerabilities in the Internet telephony domain, Bell Labs Technical Journal 12 (3) (2007) 7–19.

[36] J.F. Hair Jr., W.C. Black, B.J. Babin, R.E. Anderson, R.L. Tatham, Multivariate Data Analysis, 6th ed., Prentice Hall, Upper Saddle, 2006.

[37] Harris Interactive, Online Security and Privacy Study, http://www.whitehouse.gov/files/documents/cyber/National%20Cyber%20Security%20Alliance%20-%20Harris+Online+Security+and+Privacy+Study.pdf (Accessed 18 August 2012).

[38] J.B. Heide, G. John, The role of dependence balancing in safeguarding transaction-specific assets in conventional channels, Journal of Marketing 56 (January) (1988) 20–35.

[39] D.L. Hoffman, T.P. Novak, M.A. Peralta, Information privacy in the marketspace: implications for the commercial uses of anonymity on the web, The Information Society 15 (2) (1999) 129–140.

[40] L.T. Hu, P.M. Bentler, Fit indices in covariance structure modeling: sensitivity to underparameterization model misspecification, Psychological Methods 3 (1998) 424–453.

[41] C.B. Jarvis, S.B. MacKenzie, P.M. Podsakoff, A critical review of construct indicators and measurement model misspecification in marketing and consumer research, Journal of Consumer Research 30 (2) (2003) 199–218.

[42] S. Jayachandran, S. Sharma, P. Kaufman, P. Raman, The role of relational information processes and technology use in customer relationship management, Journal of Marketing 69 (2005) 177–192.

[43] M. Keil, H.K. Lee, T. Deng, Understanding the most critical skills for managing IT projects: a Delphi study of IT project managers, Information Management 50 (7) (2013) 398–414.

[44] M.Y. Kiang, Q. Ye, Y. Hao, M. Chen, Y. Li, A service-oriented analysis of online product classification methods, Decision Support Systems 51 (1) (2011) 28–39.

[45] D.J. Kim, D.L. Ferrin, H.R. Rao, A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents, Decision Support Systems 44 (2) (2008) 544–564.

[46] C. Kim, W. Tao, N. Shin, K.S. Kim, An empirical study of customers' perceptions of security and trust in e-payment systems, Electronic Commerce Research and Applications 9 (2010) 84–95.

[47] J.W. Lian, T.M. Lin, Effects of consumer characteristics on their acceptance of online shopping: comparisons among different product types, Computers in Human Behavior 24 (2008) 48–65.

[48] Z. Liao, W.K. Wong, The determinants of customer interactions with Internet-enabled e-banking services, Working Paper No. 0701, Department of Economics, National University of Singapore, 2007.

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

[50] L. Liu, C. Li, S.J. Karau, A measurement model of trust in Internet stores, 2nd International Conference on Electronic Business, 2002, Taipei, Taiwan.

[51] C.S. Lu, K.H. Lai, T.C.E. Cheng, Application of structural equation modeling to evaluate the intention of shippers to use Internet services in liner shipping, European Journal of Operational Research 180 (2007) 845–867.

[52] W. McFadzean, J.N. Ezingeard, D. Birchall, Information assurance and corporate strategy: a Delphi study of choices, challenges, and developments for the future, Information Systems Management 28 (2) (2011) 102–129.

[53] V.L. Mitchell, Knowledge integration and information technology project performance, MIS Quarterly 30 (4) (2006) 919–939.

[54] A. Motro, A unified model for security and integrity in relational database, Journal of Computer Security 1 (1992) 189–213.

[55] T. Noordewier, G. John, J. Nevin, Performance outcomes of purchasing arrangements in industrial buyer–seller relationships, Journal of Marketing 54 (1990) 80–93.

[56] J.C. Nunnally, Psychometric Theory, McGraw-Hill, New York, 1978.

[57] A. O'Cass, T. Fenech, Web retailing adoption: exploring the nature of Internet users web retailing behavior, Journal of Retailing and Consumer Services 10 (2003) 81–94.

[58] Office of Fair Trading (OFT), Findings from consumer surveys on Internet shopping: a comparison of pre and post study consumer research, http://www.oft.gov.uk/shared_oft/reports/Evaluating-OFTs-work/oft1079.pdf (Accessed 18 August 2012).

[59] M. Parent, The 6th and biggest lie of all: lessons from a decade of e-tailing, Ivey Business Journal Online 71 (8) (2007) 1–7.

[60] S. Petter, D. Straub, A. Rai, Specifying formative constructs in information systems research, MIS Quarterly 31 (4) (2007) 623–656.

[61] P. Podsakoff, D. Organ, Self-reports in organizational research: problems and prospects, Journal of Management 12 (1986) 531–544.

[62] G. Ramani, V. Kumar, Interaction orientation and firm performance, Journal of Marketing 72 (2008) 27–45.

[63] S. Ransbotham, S. Mitra, J. Ramsey, Are markets for vulnerabilities effective? MIS Quarterly 36 (1) (2012) 43–64.

[64] J.C. Roca, J.J. García, J.J. de la Vega, The importance of perceived trust, security and privacy in online trading systems, Information Management & Computer Security 17 (2) (2009) 96–113.

[65] J.J. Ryan, D.J. Ryan, Proportional hazards in information security [electronic version], Risk Analysis: An International Journal 25 (2005) 141–149.

[66] W.D. Salisbury, R.A. Pearson, A.W. Pearson, D.W. Miller, Perceived security and World Wide Web purchase intention, Industrial Management & Data Systems 101 (2001) 165–176.
[67] G.P. Schneider, Electronic Commerce, 9th ed., Cengage Learning, 2010.
[68] R. Sethi, Z. Iqbal, Stage-gate controls, learning failure, and adverse effect on novel new products, Journal of Marketing 72 (2008) 118–134.
[69] D.H. Shin, Ubiquitous computing acceptance model: end user concern about security, privacy and risk, International Journal of Mobile Communications 8 (2) (2010) 169–186.
[70] J. Simpson, C. Paul, The combined effects of dependence and relationalism on the use of influence in marketing distribution systems, Marketing Letters 5 (2) (1994) 153–163.
[71] M.T. Siponen, H. Oinas-Kukkonen, A review of information security issues and respective research contributions, The Database for Advances in Information Systems 38 (2007) 60–80.
[72] J.B.E.M. Steenkamp, H.C.M. Van Trijp, The use of LISREL in validating marketing constructs, International Journal of Research in Marketing 8 (1991) 283–299.
[73] E. Swilley, Technology rejection: the case of the wallet phone, Journal of Consumer Marketing 27 (4) (2010) 304–312.
[74] G. Torkzadeh, J.C.J. Chang, G.W. Hansen, Identifying issues in customer relationship management at Merck — Medco, Decision Support Systems 42 (2) (2006) 1116–1130.
[75] T. Tsiakis, G. Sthephanides, The concept of security and trust in electronic payments, Journal of Computer Security 24 (2005) 10–15.
[76] A. Usoro, S. Shoyelu, M. Koufie, Task-technology fit and technology acceptance models applicability to e-tourism, Journal of Economic Development, Management, IT, Finance and Marketing 2 (1) (2010) 1–32.
[77] G. Vaidyanathan, S. Mautone, Security in dynamic web content management systems applications, Communications of the ACM 52 (12) (2009) 121–125.
[78] B. Vatanasombut, M. Igbaria, A.C. Stylianou, W. Rodgers, Information systems continuance intention of web-based applications customers: the case of online banking, Information & Management 45 (2008) 419–428.
[79] W.F. Velicer, J.L. Fava, Effects of variable and subject sampling on factor pattern recovery, Psychological Methods 3 (1998) 231–251.
[80] M.M. Yenisey, A.A. Ozok, G. Salvendy, Perceived security determinants in e-commerce among Turkish university students, Behaviour & Information Technology 24 (2005) 259–274.
[81] S. Yousafzai, J. Pallister, G. Foxhall, Multi-dimensional role of trust in Internet banking adoption, The Service Industries Journal 29 (5–6) (2009) 591–605

Dr. Edward Hartono is an Assistant Professor of Management Information Systems in the Lerner College of Business at the University of Delaware. He received his Ph.D. in Decision Sciences and Information Systems from the University of Kentucky. His research focuses on e-commerce, IT implementation, and IT-supported collaboration. His research has appeared in Decision Support Systems, MIS Quarterly, Information and Management, DATABASE for Advances in Information Systems, and Information Systems and e-Business Management.

Dr. Clyde W. Holsapple, a Fellow of the Decision Sciences Institute, holds the Rosenthal Endowed Chair in the University of Kentucky's Gatton College of Business. He has authored more than 150 articles in journals including Decision Support Systems, Decision Sciences, Operations Research, Journal of Operations Management, Organization Science, Journal of Management Information Systems, and Journal of Strategic Information Systems. His books include Handbook on Knowledge Management, Foundations of Decision Support Systems, and Handbook on Decision Support Systems.

Dr. Ki-Yoon Kim is a Professor of Management Information Systems and the Chairman of the Department of Business Administration at Kwangwoon University, Seoul, Korea. His research focuses on security management, and software and information system risk management. He received his Ph.D. in Management Science at the Korea University in Korea.

Dr. Kwan-Sik Na is a Professor of Management Information Systems at the Seowon University in Korea. He received his Ph.D. in Management Information Systems and Management Science at the Kwangwoon University in Korea. His research focuses on Supply-chain Management, Inter-organizational Systems, Software and Information System Risk Management, Decision Support Systems, and Software Industry Research. He has published over 40 articles in various journals including the International Journal of Information Management, Cluster Computing, and Journal of Systems and Software.

Dr. James T. Simpson was a Distinguished Professor of Marketing and Dean of the College of Business Administration at the University of Alabama in Huntsville. He received his Ph. D. in Marketing and Applied Statistics at the University of Alabama. His research focuses on technology management, marketing high technology product and services, and Journal of Systems and Software, and Cluster Computing, and marketing channel structure and behavior. His research has appeared in numerous journals including the Journal of Marketing Research, Marketing Letters, Journal of Business Research, Journal of Systems and Software, and European Journal of Innovation Management. He has served as Director of the UAH Center for the Management of Science and Technology, and has lectured and served as a visiting scholar at universities in Russia, France, China, Romania, Taiwan, Ireland and England.