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.

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/

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