8-5-2011

Understanding the Security in Privacy-Security Concerns: A Theoretical and Empirical Examination

Gaurav Bansal
University of Wisconsin - Green Bay, bansalg@uwgb.edu

Understanding the Security in Privacy-Security Concerns: A Theoretical and Empirical Examination

Gaurav Bansal
Austin E. Cofrin School of Business
University of Wisconsin - Green Bay
bansalg@uwgb.edu

ABSTRACT

Even though Privacy concerns and security concerns are acknowledged as separate constructs, many studies argue that they are related or, even worse, confused. Hence, this study clarifies the nuances between privacy and security concerns, and identifies the dimensions which pertain purely to the security side. It develops a scale to measure those "security dimensions". It shows that unique dimensions relate to the transmission aspect of security concern. Hence we call this scale Internet Users Information Transmission Security Concern (IUITSC) scale. This study draws upon a sample of 270 Internet users to validate and empirically examine the factor structure of the scale. The results suggest that IUITSC may be represented as a second-order factor structure rather than a set of four first-order factors. The study argues that *assurance* could be the overarching theme which ties the first-order dimensions of security concern into the higher order IUITSC construct. The paper most importantly, theoretically and empirically establishes the distinctness of the IUITSC scale with privacy concern dimensions. Together the IUITSC and privacy concern dimensions cover the entire gamut of privacy-security concerns.

Keywords

Privacy concern, Security concern, IUITSC, Internet users' information transmission security concerns

INTRODUCTION

There is compelling evidence that ecommerce is growing rapidly despite the dismal economy in recent years. According to the eMarketer (Plunkett Research 2010), ecommerce sales for 2010 reached $152.1 billion. Even though this is a meager 3.87% of retail sales, it is a notch higher than 3.3% for 2008 (Hu et al. 2010). These numbers suggest that ecommerce is growing, but has definitely not reached its full potential yet. A survey conducted by PEW in May 2010 (Plunkett Research 2010) suggests that 78% of U.S. adults use the Internet to research a service or product they are interested in buying; and Digital Future (2010) suggest that only 65% actually buy anything online. The PEW survey also reveals that only 58% of Internet users do banking online. To reach its full potential, ecommerce must overcome many challenges (Hu et al. 2010), and one of them is definitely Internet Security Concerns (SC).

The Digital Future (2010) report suggests that security concerns remain near the all-time high. These concerns result from the fear of harmful economic and social consequences that might result from the misuse of private information disclosed in online transactions (Bansal and Zahedi 2010). It is reported that 75% percent of U.S. adults are at least somewhat concerned about Internet security where as 65% are extremely concerned about misuse of their personal information (PCWorld.com 2009). This trust could hamper the development of cloud computing and third party data hosting among others.

We build upon Bansal and Zahedi (2010), to contrast SC and Privacy concerns (PC). We identify the unique SC dimensions which do not overlap with PC. As explained below, all these dimensions relate to the transmission aspect of security concern. We then develop a scale to measure those dimensions. Hence we call this scale Internet Users Information Transmission Security Concern (IUITSC) scale. Together the IUITSC dimensions along with PC scale cover the entire gamut of SC-PC. We follow the guidelines suggested by Stewart and Segars (2002) in examining the factor structure of the newly developed IUITSC scale - first order versus second order. We contrast various combinations: one first-order, two first-orders, three first-orders, four first-orders and a second-order factor model for IUITSC. We then examine the best fitting models in the nomological network to further examine the empirical properties of the models. We rely on confirmatory factor analysis to identify the best factor structure for IUITSC. However, we also use EFA to supplement the analysis at various levels. As suggested by Smith et al. (1996), as part of establishing the discriminant validity of IUITSC, we contrast the IUITSC scale

with CFIP (PC scale) - as set of first order dimensions (Smith et al. 1996) and as a second order construct (Stewart and Segars 2002).

This paper contributes to the field in the following ways. First, the paper develops and rigorously validates an instrument to measure IUITSC. Second, it suggests that IUITSC may be represented as a second-order factor structure. Third, it argues that *assurance* could be the overarching theme which ties the four first factor security concern dimensions into the higher order IUITSC construct. The paper most importantly, theoretically and empirically, establishes the distinctness of IUITSC scale with privacy concern dimensions. The importance of this scale is that it builds upon the non-overlapping dimensions of privacy concern, hence, when used in conjunction with the PC scale it covers all the dimensions of information security and privacy.

The paper is organized as follows. We develop the theoretical foundation for multiple factor structures including various combinations of first order factor models as well as the second order factor model. We then provide an overview of research methodology. Results are presented next, followed by discussion and conclusion.

THEORETICAL FOUNDATIONS AND ALTERNATIVE MODELS OF IUITSC

The concept of security concern is being discussed in IS since 1983 (e.g. Benson 1983, Goodhue and Straub 1991, Loch et al. 1992, White and Christy 1987), however, only recently have there been attempts to empirically examine the user's security concerns. Table 1 provides a brief overview of the salient literature in this area, and also reflects that the four-dimension model of SC comprised of authentication, confidentiality, integrity and non-repudiation has gained wide acceptance.

Source	Security Construct Conceptualization	Type of Study	Factor Structure
Bansal and Zahedi (2010)	Four dimensions: Authentication, Confidentiality, Integrity and Nonrepudiation	Theoretical argument	
Chellappa and Pavlou (2002)	One dimension comprised of items related to: Authentication, Authorization (Confidentiality), and Non-repudiation (Integrity)	Empirical study	One first order factor comprised of 5 items
Flavian and Guinaliu (2006), Casalo et al. (2007)	One dimension	Empirical study	One first order factor comprised of 8 items
Kim 2008	One dimension	Empirical study	One first order factor comprised of 4 items
Pavlou et al. 2007	One dimension	Empirical study	One first order factor comprised of 5 items.
Ratnasingam et al. 2005	Four dimensions: Authenticity, Confidentiality, Integrity, and Non-repudiation	Theoretical argument	
Salisbury et al. 2001	One dimension	Empirical study	One first order factor comprised of 7 items
Smith et al. (2011)	Three dimensions: Authentication, Confidentiality, and Integrity	Theoretical argument	

Table 1. Conceptualization of Security Concern in Literature

Before we start delving into measuring SC, we would first like to understand what SC is and what it is not. Even though PC and SC are acknowledged as separate constructs (Pavlou et al. 2007), many studies argue that they are related or, even worse, confused (Casalo et al. 2007). "Little consensus exists on the distinction between PC and SC" (Bansal and Zahedi 2010, p. 2). It is thought that PC are the beliefs of the users regarding the protection of the data while it is in stored on the website's end, whereas SC pertain to the data in the transmission as well as the storage state (Bansal and Zahedi 2010).

Table 2 provides a list of the four privacy dimensions (Smith et al. 1996) and the four security dimensions (Bansal and Zahedi 2010), their descriptions and their characteristics.

S.No.	Concern Dimension		Description	Privacy concern	Security concern	Transmission / Storage	Management's Role
#1	Collection		Collecting too much user information	X		Storage	Willful
#2	Unauthorized secondary use		Using the information for other purposes without prior approval of the user	X		Storage	Willful
#3a	Error (Integrity)	Transmission related	Preventing the data from getting corrupted		X	Transmission	Inability or unwillingness
#3b		Storage related		X	X	Storage	Inability or unwillingness
#4a	Improper Access (Confidentiality or unauthorized access)	Transmission related	Hiding the information from unauthorized viewing		X	Transmission	Inability or unwillingness
#4b		Storage related		X	X	Storage	Inability or unwillingness
#5	Authentication		Verification of the correct user and the website		X	Transmission	Inability or unwillingness
#6	Nonrepudiation		Obtaining the receipt of the transaction		X	Transmission	Inability or unwillingness

Table 2. Contrasting Privacy and Security Concerns

In Table 2, dimensions #1, #2, #3b, and #4b are PC dimensions, and #3 (a and b), #4 (a and b), #5, and #6 pertain to SC. Dimensions #1 and #2 are result of website's willful intentions and ethics (Yang et al. 2009) in handling data, and the rest could be argued to relate to website's inability or unwillingness to safeguard the data. Bansal and Zahedi (2010) argued that PC and SC overlap for #3b and #4b, as they both are storage related. They also maintained that the dimensions #3a, #4a, #5 and #6 are unique to SC, whereas #1 and #2 are unique to PC. Definition-wise, *errors* in PC is similar to *integrity* in SC. Likewise, *improper access* in PC is similar to *confidentiality* or *unauthorized access* in SC. Hence, we have grouped them together as #3 and #4 in Table 2.

In this study we develop an instrument to measure the unique dimensions (highlighted in grey cells in Table 2) of SC (#3a, #4a, #5, #6), which do not overlap with PC. Interestingly, we find that all these dimensions are transmission related. Accordingly, we categorize them as Internet users' information transmission security concerns (IUITSC). Basing our definition of IUITSC on Pavlou et al. (2007), we define it as the user's beliefs about the website's inability or unwillingness to safeguard information from security breaches during transmission over the World Wide Web.

The scale is important, as when used in conjunction with the PC scale it covers all the information concern dimensions (#1 thru #6).

As per the guidelines suggested by Stewart and Segars (2002) we first examine various models that have been proposed as plausible representations of the IUITSC phenomenon. The following sections describe the theoretical and operational details of the five models identified for the analysis.

First-Order IUITSC Models

Model 1 hypothesizes one first-order factor for IUITSC. Table 1 lists several studies that have specifically assessed information security concern as a one dimension first-order model. This would be similar to Chellappa and Pavlou (2002).

Model 2 hypothesizes that the items form two first-order factors. This model proposes that Internet users divide their concerns into two primary areas: privacy related (confidentiality, and integrity) and security related (authentication, and non-repudiation).

Model 3 hypothesizes that items form three first-order factors. A recent study (Pilcher 2010) suggested that consumers are most concerned about three security concerns namely id theft, phishing and privacy. Developing three factors along these lines we associated authentication with id theft, nonrepudiation with phishing, and integrity and unauthorized access with privacy.

Model 4 hypothesizes that the items form four first-order factors. Model 4 implies that every item is equally important in computing each factor and each factor is equally important in estimating the higher-order construct (Stewart and Segars 2002).

A Second-Order Factor Model

Model 5 hypothesizes that the items form four first-order factors and that these four first-order factors are measured by a second-order factor IUITSC. According to Stewart and Segars (2002) in such higher-order models the intercorrelations among first-order factors form a system of interdependence. They contend that this interdependence is important in measuring the higher-order construct. Therefore, when conceptualizing IUITSC as a second-order factor model, it is viewed as a set of four distinct factors as well as the structure of interrelationships among those factors.

While users' security concerns may relate to very specific information practices such as non-repudiation, authentication, integrity, and unauthorized access, the overarching concern that accounts for the interdependencies among these factors may be the degree of *assurance* or the *control* over their personal information that is retained by the organization/website. This *control* is very much different from the *control* in PC. In SC users desire the organization to have control over their information and protect it from criminals/hackers, who are intentionally trying to get to the information. Whereas, in PC, the users themselves want to exercise control (Stewart and Segars 2002, Smith et al. 2011), however small, over the information.

RESEARCH METHODOLOGY

Data for model testing was obtained through a lab experiment conducted using participants who were students in a Midwestern university. A total of 270 observations were used in the analysis. The demographics are presented in Table 3. Two respondents did not disclose their gender. They had an average of 20 years of internet experience (std dev = 12.668 years) and an average of 7.844 years of online social networking experience (std dev = 5.200 years).

Gender	Number	Age range Years	Average Age Years	Standard Deviation (Years)
Males	122	19 to 55	22.918	5.427
Females	146	19 to 31	21.020	1.943

Table 3. Demographics

Consistent with work of Stewart and Segars (2002) confirmatory factor analysis (CFA) was utilized to assess the efficacy of the theorized models. CFA estimations were done with MPlus 4.1 (Muthen and Muthen 2007). The estimation used the mean-adjusted maximum likelihood, which adjusts the estimation result for the non-normality in data.

RESULTS

Table 4 provides a summary of the model-fit measures observed for the various models. As shown, the first three models have a high chi square / df ratio, low CFI and TLI, and high RMSE and SRMR values indicating poor model fit. The fit indices (Table 4) indicate that Model 4 (four first-order factors) and Model 5 (a second-order factor model) exhibit much stronger measures of fit than any of the other hypothesized models. Therefore, we further consider the properties of these models. In Table 5 we provide the results of the CFA analysis of the models 5 and 6.

	Model 1 One first-order factor	Model 2 Two first-order factors	Model 3 Three first-order factors	Model 4 Four first-order factors	Model 5 Second-order factor	Thresholds (Source: Song and Zahedi 2005)
Chi-sq (df)	1072.260 (35)	624.156 (34)	413.515 (32)	64.538 (29)	74.414 (31)	
Chi-sq/df	30.636	18.358	12.922	2.225	2.400	< 3.00 or < 5.00
CFI	.633	.791	.865	.987	.985	>.900
TLI	.529	.724	.810	.981	.978	>.900
RMSEA	.331	.254	.210	.067	.072	<.060
SRMR	.116	.131	.094	.023	.031	<.100

Table 4. Fit indices of various models

		Four First-Order Factors		Second-Order Factor Model		
		Factor Loading	T- Value		Factor Loading	T - Value
Authenticity	ASC3	0.921	40.888	ASC3	0.921	40.305
	ASC1	0.858	34.276	ASC1	0.857	33.785
Confidentiality†	UASC1	0.948	110.047	UASC1	0.948	110.191
	UASC2	0.936	98.138	UASC2	0.936	97.797
	UASC3	0.945	106.514	UASC3	0.945	106.014
Integrity†	ISC2	0.965	76.143	ISC2	0.965	73.499
	ISC1	0.931	65.741	ISC1	0.931	64.163
Non-repudiation	NRSC1	0.896	59.974	NRSC1	0.896	60.104
	NRSC2	0.940	85.412	NRSC2	0.939	84.638
	NRSC3	0.913	70.216	NRSC3	0.913	70.121
IUITSC				ISC	0.850	30.231
				UASC	0.798	25.962
				ASC	0.792	22.659
				NRSC	0.781	23.700

Table 5. CFA analysis for models 4 and 5

†Transmission related

The standardized factor loadings for both the models range between .781 and .965. The two tail T-values are all higher than 1.96, thus providing evidence to support the convergent validity of the items measured (Anderson and Gerbing 1988). We initially started with 11 items (refer to Appendix A). Item ASC 2 was dropped because of low factor loading. We conducted the EFA analysis of the 10 newly developed IUITSC items organized as four first-order factors. The results are presented in Appendix B. All the factor loadings are higher than .81, and no cross loadings greater than .40 are observed. We also performed EFA with the IUITSC (set of four first order dimensions: authenticity, confidentiality, integrity, non-repudiation) and PC (set of four first-order factors: collection, error, improper access and unauthorized secondary use) items together. The results are provided in Appendix C. The EFA factor loadings are all greater than .78, and there are no cross-loadings greater than .40. We also performed CFA analysis for the eight dimensions. The CFA factor loadings range from .858 to .976 and T-values are all more than 35.368. To further validate the convergent and discriminant validity we performed CFA of PC and IUITSC factoring both as second-order factor models. The T-values ranged from 4.412 to 29.272. The factor loadings for all

four IUITSC dimensions and two PC dimensions (secondary use and collection) were greater than .75, however, the factor loadings for two PC dimensions, unauthorized access and errors, were .48 and .29 respectively. The fit indices are reported in Table 6 below. This exercise further validates the claim by Bansal and Zahedi (2010) that PC and SC are distinct constructs and also validates the convergent and discriminant validity of the IUITSC items with regard to the PC items. Further inquiry is necessary to investigate the low factor loadings for unauthorized access and errors when PC and IUITSC were factored in as second-order factor models.

	PC and IUITSC Each as a set of four first-order factors	PC and IUITSC Each as a second-order factor model	Thresholds (Source: Song and Zahedi 2005)
Chi sq (df)	701.107 (182)	455.961 (200)	
Ch sq / df	3.852	2.28	<3.00 or <5.00
CFI	.919	.960	>.900
TLI	.897	.954	>.900
RMSEA	.103	.069	<.060
SRMR	.131	.110	<.100

Table 6. Fit indices of CFA conducted with PC and SC items together

Placing IUITSC within a Nomological Network

Along the lines of Stewart and Segars (2002) we further compare the IUITSC as a first-order and second-order factor model within a nomological network. Developing the nomological network we would like to argue that IUITSC, similar to PC, would mediate the users' personal dispositions and their attitude towards the use of technology (Smith et al. 1996, Bansal et al. 2010). Bansal et al. (2010) established that emotional instability is positively associated with information sensitivity. Emotional instability is associated with being anxious, depressed, stressed, suggestible, volatile, and fearful (Goldberg 1992). We argue that those who are anxious are more likely to be more nervous about their private information and should, therefore, have higher information security concern. Hence, we argue that emotional instability would be negatively associated with IUITSC. From the standpoint of predictor variables, individuals that exhibit high levels of IUITSC are less likely to trust a website. Prior studies have argued that privacy concerns negatively impact trust in a website (e.g., Bansal et al. 2010). Those who are more concerned about their information privacy and security would also have more reasons to mistrust a particular website. In the same vein it could be argued that the IUITSC would negatively affect trust in a website. Using previously defined scales for emotional instability (EMN) and trust (TRU) we expand the analysis of IUITSC (Table 7).

Construct	Items	Source
	On a scale of 0 - 10	
Trust	I believe that this *website* is (not honest at all / very honest) (not reliable at all / very reliable) (opportunistic / dependable) The level of my trust for this website is (very low / very high)	Gefen et al. 2003
Emotional Instability	I often feel blue (strongly disagree / strongly agree) I get stressed out easily (strongly disagree / strongly agree) I am easily disturbed (strongly disagree / strongly agree) I get upset easily (strongly disagree / strongly agree) I change mood a lot (strongly disagree / strongly agree) I get irritated easily (strongly disagree / strongly agree)	Fraj and Martinez 2006, Goldberg 1992

Table 7. Instrument for nomological network

Three corporate and three facebook websites ranging in different trust levels were identified. Each participant was randomly assigned to view one of the six websites. Each participant was asked to respond to a series of questions pertaining to the trust in the website and their personal characteristics (IUITSC, PC, EMN, demographics). We first performed the reliability analysis, which is presented in Table 8. Cronbach alpha and CFR values are higher than the suggested threshold. We also performed Harman's single factor test to examine the common method variance. The first factor explained 34.7% of the variance, thus suggesting that the common method variance does not pose a serious problem.

Construct	Cronbach Alpha	CFR
Authentication	.883	.884
Confidentiality	.960	.960
Integrity	.959	.947
Non repudiation	.938	.940
Emotional instability	.900	.899
Trust	.931	.776
IUITSC (as second-order construct)	-	.881

Table 8. Reliability

Figure1 illustrates model 6 and the associated path coefficients of IUITISC as a set of first-orders that mediate the relationship between emotional instability and trust. Figure 2 illustrates model 7 and the associated path coefficients of IUITSC as a second-order factor model mediating the relationship between emotional instability and trust.

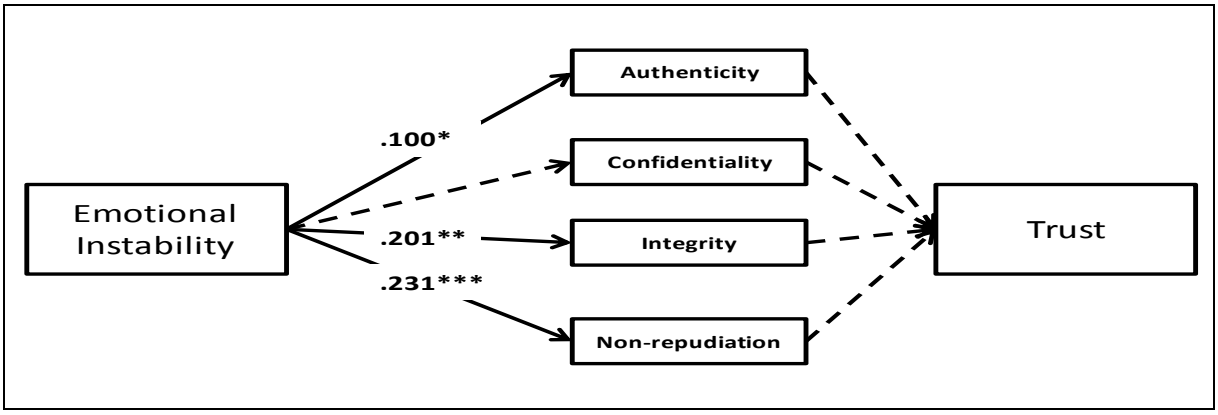

Figure 1. IUITSC Nomological network: First-order (Model 6)

<>

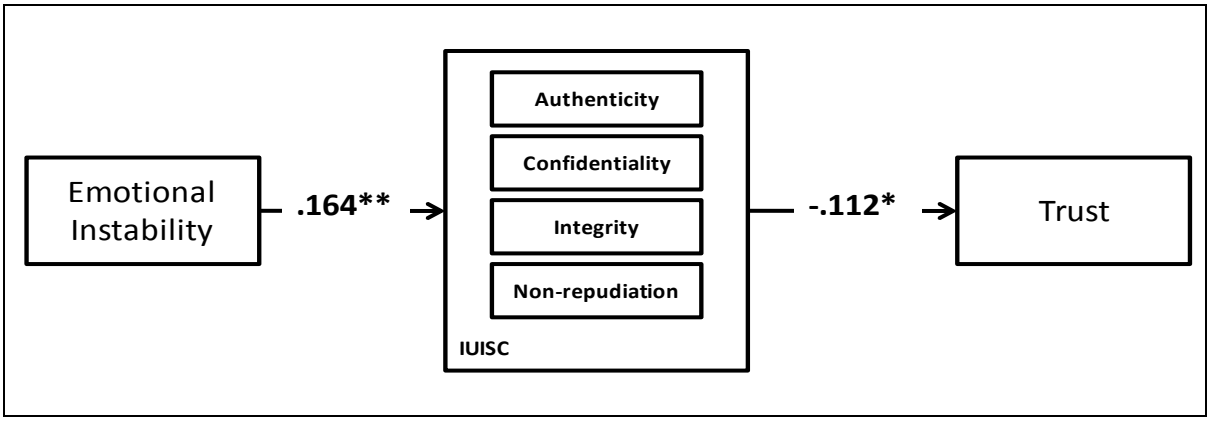

Figure 2. IUITSC nomological network: Second-order (Model 7)

Table 9 outlines the observed chi-square and fit indices of models 6 and 7. As shown, the fit indices for model 6 are somewhat lower than those observed for Model 7 due to factor and item complexity (more items more factors).

Fit Indices	**Model 6** IUITSC as first-order factor model mediating within the nomological net	**Model 7** IUITSC as second-order factor mediating within the nomological net	**Thresholds** (Source: Song and Zahedi 2005)
Chi sq (df)	788.943 (162)	333.170 (164)	
Ch sq / df	4.870	2.03	< 3.00 or < 5.00
CFI	.868	.964	>.900
TLI	.846	.959	>.900
RMSEA	.120	.062	<.060
SRMR	.222	.052	<.100

Table 9. IUITSC within nomological network

When compared to model 6, model 7 seems to provide a better fit. In addition, the path coefficients between IUITSC as second-order factor model and the predictor and consequent constructs are much higher and significant than the estimated paths of the first-order model.

	1	2	3	4	5	6	7	AVE
Confidentiality (1)	**0.943***							0.889
Integrity (2)	0.679	**0.949***						0.900
Authentication (3)	0.624	0.675	**0.890***					0.792
Non-repudiation (4)	0.623	0.675	0.620	**0.916***				0.839
IUITSC (5)	0.792	0.857	0.788	0.787	**0.807***			0.651
Trust (6)	-0.089	-0.096	-0.088	-0.088	-0.112	**0.946***		0.894
Emotional Instability (7)	0.130	0.141	0.130	0.129	0.164	-0.018	**0.774***	0.599

Table 10. Correlations, AVE, and square root of AVE
(*The diagonal bold values are square root of AVE)

Table 10 shows the AVE and construct correlations among the IUITSC, the four security concern dimensions, along with trust (TRU) and emotional instability (EMN). EMN, TRU and IUITSC have lower correlations among themselves (grey shaded cells in the Table 10) than the corresponding square root of AVE values. The four SC dimensions share high correlations with the second order IUITSC construct (non-grey cells in the Table 10). This provides rigorous support to the discriminant and convergent validity of the IUITSC construct (Song and Zahedi 2005).

Given the theoretical and empirical support for the second-order construct, these results seem to confirm the conceptualization of IUITSC as a second-order factor structure.

DISCUSSION AND CONCLUSION

The results of this study provide interesting insights into the dimensionality of the IUITSC construct. Limitations of the study, however, should be noted. The data was obtained from undergraduate students, hence in order to increase the generalizability the study should be replicated with different data sets and contexts.

The results of this study enhance our understanding of the nature and dimensionality of the IUITSC construct. We find the IUITSC construct to be well measured by first-order constructs of non repudiation, unauthorized access, authentication and integrity. We also find empirical support for the theorized second-order factor of IUITSC.

Another important contribution of this paper lies in the fact that it systematically studies the differences between SC and PC. Many studies have argued that privacy and security are two different constructs and "the two need to be handled as distinct concepts" (Flavian and Guinaliu 2006, p. 605), however, none has distinguished them thus, theoretically and empirically.

The results indicate that when it comes to transmission related security concerns on the world wide web, consumers are concerned about all four issues: authenticity, confidentiality, integrity and nonrepudiation. The results also suggest that the interrelationship among these factors is an important component of accurately measuring IUITSC. Stewart and Segars (2002) argued that failing to model a higher-order factor accordingly can result in inaccurate findings by neglecting to account for the common variation explained by the interdependencies among the four first-order factors. They also advised on working with appropriate model, as modeling a set of constructs as an aggregate composite leads to different results than the modeling of constructs as reflective of a higher-order factor (Bollen and Lennox 1991).

The recent disclosure about security attacks on Google (WSJ January 19, 2010) and 2,411 other firms (WSJ February 18, 2010) has heightened the awareness of consumers in security issues. As noted earlier, a central concern that seems to underlie consumer attitudes, and is perhaps the common theme captured by the higher-order concept of IUITSC, is the issue of assurance. As opposed to privacy concern, where consumers desire control over the information, here the consumers desire that the entity collecting the information exercises control over the information and assures it against unintended consequences. Understanding consumer concerns regarding information security is important to practitioners as well. Corporations can use the results for their policymaking efforts. For researchers the scale is important, as when used in conjunction with PC scale it would cover all the information concern dimensions: collection, unauthorized secondary use, improper access, errors, authentication, and nonrepudiation (dimensions #1 thru #6 mentioned in Table 2).

In this study we examined the dimensions which were unique to SC, and did not theoretically overlap with PC. Future research could differentiate the PC and SC from overlapping areas such as errors and improper access during the storage phase. The clarification would benefit the IS community as several papers treat employee browsing as a security breach (Dhillon 2001, Warkentin and Willison 2009), and some treat data breach as privacy loss (Culnan and Williams 2009).

REFERENCES

1. Anderson, J. and Gerbing, D. (1988) Some methods for respecifying measurement models to obtain uni-dimensional construct measurement, *Journal of Marketing Research*, 19, 4, 453-460.
2. Bansal, G. and Zahedi, F. M. (2010) Trading Trust for Discount: Does Frugality Moderate the Impact of Privacy and Security Concerns? in proceedings of the *16th Americas Conference on Information Systems*, Peru.
3. Bansal, G., Zahedi F.M. and Gefen, D. (2010) The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online, *Decision Support Systems*, 49, 2010, 138-150.
4. Benson, D. (1983) A Field Study of End User Computing: Findings and Issues, *MIS Quarterly*, 7, 4, 35-45.
5. Bollen, K. A., and Lennox, R. (1991). Conventional Wisdom on Measurement: A Structural Equation Perspective, *Psychological Bulletin*, 110, 305-314.
6. Casalo, L., Flavian, C. and Guinaliu, M. (2007) The impact of participation in virtual brand communities on consumer trust and loyalty, *Online Information Review*, 31, 6, 775-792.
7. Chellappa, R. K. and Pavlou, P. (2002) Perceived information security, financial liability, and consumer trust in electronic commerce transaction, *Journal of Logistics Information Management*, 15, 5/6, 358-368.
8. Culnan, M.J., and Williams, C.C. (2009) How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches, *MIS Quarterly*, 33, 4, 673-687.
9. Dhillon, G. (2001) Violation of safeguards by trusted personnel and understanding related information security concerns, *Computers & Security*, 20, 2, 165-172.
10. Digital Future Project 2010, available at: http://www.digitalcenter.org/pdf/2010_digital_future_final_release.pdf [last accessed Feb 23, 2011].
11. Flavián,C. and Guinalíu,M. (2006) Consumer trust, perceived security and privacy policy, *Industrial Management & Data Systems*,106,5,601-620.
12. Fraj, E., and Martinez, E. (2006) Influence of personality on ecological consumer behavior, *Journal of Consumer Behavior*, 5, 167-181.
13. Gefen, D, Karahanna, E., and Straub, D.W. (2003). Trust and TAM in online shopping: An integrated model, *MIS Quarterly* 27, 1, 51-90.
14. Goldberg, L.R. (1992) The development of the markers for the big-five factor structure, *Psychological Assessment* 4, 1, 26-42.
15. Goodhue, D.L., and Straub, D.W. (1991) Security concerns of system users: a study of perceptions of the adequacy of security, *Information and Management*, 20, 1, 13-27.

16. Hu, X., Wu, G., Wu, Y., and Zhang, H. (2010) The effects of Web assurance seals on consumers' initial trust in an online vendor: A functional perspective, *Decision Support Systems*, 48, 407-418.
17. Kim, D.J., Steinfield, C, and Lai-Y-J. (2008) Revisiting the role of web assurance seals in business-to-consumer electronic commerce, *Decision Support Systems*, 44, 1000-1015.
18. Loch, K.D., Carr, H.H., and Warkentin, M.E. (1992) Threats to information systems: today's reality, yesterday's understandings, *MIS Quarterly*, 16, 2, 173-186.
19. Muthén, L.K., and Muthén, B.O. (2007) Mplus Statistical Analysis with Latent Variables (Version 4.1), *Muthén & Muthén*, Los Angeles, CA.
20. Pavlou, P. A., Lian, H. and Xue, Y. (2007) Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective, *MIS Quarterly*, 31, 1, 105-136.
21. PCWorld.com (2009) http://www.pcworld.com/businesscenter/article/174301/trust_the_cloud_americans_say_no_way.html [last accessed Feb 23, 2011]
22. Pilcher, J. (2010) Growing use of Twitter raises customer security concerns, *ABA Banking Journal*, 102, 1, 27-28.
23. Plunket Research (2010) http://www.plunkettresearch.com/ecommerce%20internet%20technology%20market%20research/industry%20statistics [last accessed Feb 23, 2011]
24. Ratnasingam, P., Gefen, D. and Pavlou, P.A. (2005) The role of facilitating conditions and institutional trust in electronic-marketplaces, *Journal of Electronic Commerce in Organizations*, 3, 3, 69-82.
25. Salisbury,W. D., Pearson, R. A., Pearson, A. W. and Miller, D. W. (2001) Perceived security and world wide web purchase intention, *Industrial Management + Data Systems*, 101,3/4,165-176.
26. Smith, H. J., Dinev, T., and Xu, H. (2011) Information Privacy Research: An interdisciplinary review, *MIS Quarterly*, forthcoming.
27. Smith, H. J., Milberg, S. J. and Burke, S. J. (1996) Information privacy: Measuring individuals' concerns about organizational practices, *MIS Quarterly*, 20, 2, 167-196.
28. Song, J. and Zahedi, F.M. (2005) A theoretical approach to web design in e-commerce: A belief reinforcement model, *Management Science*, 51, 8,1219-1235.
29. Stewart, K. A., and Segars, A.H. (2002) An empirical examination of the concern for information privacy instrument, *Information Systems Research*,13,1,36-49.
30. Yang, M-H., Chandlrees, N., Lin, B., and Chao, H-Y (2009) The effect of perceived ethical performance of shopping websites on consumer trust, *The Journal of Computer Information Systems*, 50,1,15-24.
31. Warkentin, M., and Willison, R. (2009) Behavioral and policy issues in information systems security: The insider threat, *European Journal of Information Systems*, 18, 2, 101-105.
32. White, C. E., and Christy, D.P. (1987) The information center concept: A normative model and a study of six installations, *MIS Quarterly*, 11, 4, 451-458.

APPENDIX A. IUITSC Instrument (On a scale of 0 to 10, with 0 being very low and 10 being very high)

		The level of my concern…	
Authentication	ASC1	regarding the authenticity of the Website I am transacting with is	Very low / Very high
	ASC2 **(dropped)**	that the website I am transacting with might authenticate someone else mistaking him / her to be myself is	Very low / Very high
	ASC3	the level of my concern regarding the need to authenticate the website or the user is	Very low / Very high
Confidentiality†	UASC1	regarding the protection of my personal information from unauthorized access while sending it over the web is	Very low / Very high
	UASC2	regarding the confidentiality of my personal information while sending it over the web is	Very low / Very high
	UASC3	regarding the privacy of my personal information while sending it over the web is	Very low / Very high
Integrity†	ISC1	regarding the protection of my personal information getting altered while sending it over the web is	Very low / Very high
	ISC2	regarding the protection of my personal information getting corrupted while sending it over the web is	Very low / Very high
Non-repudiation	NRSC1	that transactions over the Web could be declared untrue is	Very low / Very high
	NRSC2	that the transactions over the Web are disputable is	Very low / Very high
	NRSC3	that the transactions over the Web are deniable is	Very low / Very high

Table A. IUITSC Instrument

†Transmission related

APPENDIX B: EFA of Security Concern

	Variable	Factor1	Factor2	Factor3	Factor4
Authentication	ASC1	0.26	0.23	-0.22	**-0.86**
	ASC3	0.28	0.29	-0.23	**-0.82**
Confidentiality†	UASC1	**0.85**	0.22	-0.30	-0.24
	UASC2	**0.89**	0.19	-0.24	-0.24
	UASC3	**0.85**	0.23	-0.32	-0.21
Integrity†	ISC1	0.31	0.31	**-0.83**	-0.22
	ISC2	0.33	0.31	**-0.82**	-0.24
	ISC3	0.31	0.35	**-0.81**	-0.20
Non-repudiation	NRSC1	0.28	**0.81**	-0.30	-0.22
	NRSC2	0.18	**0.87**	-0.26	-0.24
	NRSC3	0.17	**0.87**	-0.29	-0.18

Table B. EFA of four first-order Security Concern factors

†Transmission related

APPENDIX C: EFA of Security Concern and Privacy Concern

Construct	Variable	Factor1	Factor2	Factor3	Factor4	Factor5	Factor6	Factor7	Factor8
Authentication	ASC1	0.00	0.25	0.11	-0.25	-0.09	-0.24	0.13	**-0.83**
	ASC3	0.06	0.31	0.11	-0.29	-0.12	-0.23	0.12	**-0.78**
Confidentiality†	UASC1	0.10	0.21	0.16	**-0.83**	-0.17	-0.29	0.13	-0.20
	UASC2	0.07	0.19	0.19	**-0.86**	-0.12	-0.23	0.11	-0.21
	UASC3	0.05	0.24	0.18	**-0.82**	-0.20	-0.30	0.12	-0.16
Integrity†	ISC1	0.10	0.32	0.02	-0.29	-0.09	**-0.82**	0.11	-0.20
	ISC2	0.08	0.34	0.02	-0.31	-0.12	**-0.82**	0.07	-0.20
	ISC3	0.16	0.35	0.09	-0.27	-0.15	**-0.80**	0.11	-0.14
Non-repudiation	NRSC1	0.08	**0.81**	0.09	-0.26	-0.07	-0.28	0.11	-0.19
	NRSC2	0.13	**0.87**	0.10	-0.15	-0.04	-0.25	0.09	-0.21
	NRSC3	0.09	**0.87**	0.06	-0.16	-0.10	-0.27	0.07	-0.13
Collection	ColCon1	0.05	0.07	**0.84**	-0.18	-0.22	-0.07	0.07	-0.13
	ColCOn2	-0.01	0.07	**0.90**	-0.11	-0.32	-0.02	0.08	-0.03
	ColCon3	0.01	0.08	**0.88**	-0.12	-0.34	-0.02	0.08	-0.05
Errors	ErrCon1	**0.91**	0.10	0.01	-0.07	-0.04	-0.12	0.26	0.00
	ErrCon2	**0.90**	0.03	-0.01	-0.04	-0.06	-0.08	0.34	-0.02
	ErrCon3	**0.90**	0.14	0.06	-0.07	-0.09	-0.05	0.25	-0.04
Improper access	UACon1	0.29	0.09	0.10	-0.12	-0.14	-0.11	**0.83**	-0.11
	UACon2	0.31	0.09	0.09	-0.09	-0.12	-0.05	**0.86**	-0.13
	UACon3	0.39	0.10	0.07	-0.10	-0.16	-0.10	**0.81**	-0.02
Unauthorized secondary use	SecCon1	0.06	0.06	0.40	-0.18	**-0.81**	-0.09	0.16	-0.09
	SecCon2	0.10	0.09	0.31	-0.13	**-0.87**	-0.10	0.15	-0.02
	SecCon3	0.07	0.08	0.34	-0.13	**-0.85**	-0.13	0.13	-0.13

Table C. EFA of first-order four Privacy Concern and first-order four Security Concern factors

†Transmission related