Transactions on Replication Research

Methodological Replication DOI: 10.17705/1atrr.00069 ISSN 2473-3458

Home Computer User Security Behavioral Intention: A Replication Study from Guam

Kevin K.W. Ho

School of Business and Public Administration, University of Guam

kevinkho@triton.uog.edu

Cheuk Hang (Allen) Au

Department of Information Management, National Chung Cheng University, Taiwan

allenau@ccu.edu.tw

Dickson K.W. Chiu

Faculty of Education, The University of Hong Kong

dicksonchiu@ieee.org

Abstract:

This replication study is a methodological replication of Study 1 of Anderson and Agarwal (2010) (A&A) using data collected from Guam to investigate information security (InfoSec) behavioral intention. This study also extended the A&A Model by examining the effect of gender on each construct of the model. Our findings are very similar to those reported by A&A, and indicate that the model is generalizable to the population on Guam. We also observed the effect of gender on several constructs of the model. As this study cannot confirm whether the slight differences between the result of A&A and this study are related to cultural differences, we suggest future replication studies be conducted to examine how culture would affect our security behavior intention. We also suggest practitioners consider gender as an important factor when designing mechanisms to encourage people to practice information security behavior.

Keywords: Behavioral security, protection motivation, home computer user, survey, replication study, Guam

The manuscript was received 3/14/2020 and was with the authors for 4 months for 2 revisions.

1 Introduction

In this study, we present a replication of Study 1 of Anderson and Agarwal (2010) using data collected from Guam to investigate security behavioral intention. It is a methodological replication as we use the same methods as Anderson and Agarwal (2010) but conducted in a different location (i.e., US Mainland versus Guam) (Dennis and Valacich, 2015). This type of methodological replications conducted in different locations or countries is important for improving the generalizability of the theories (Im and Straub, 2015). Guam is selected as the focus of this study as it is a US unincorporated territory located in the West Pacific, which has a different cultural background from the Western world in which Anderson and Agarwal's study (2010) had been conducted. In particular, based on Hofstede's Cultural Dimensions score (Hofstede, 2001 Perez *et al.*, 2015), the cultural dimension scores of Guam and the US are very different in *power distance* and *masculinity*, which indicate there exists observable differences between the culture of these two places. We also extended our study by analyzing the results based on gender and investigated whether the model from Anderson and Agarwal's Study 1 (2010) would be generalized to both genders.

2 Literature Review

2.1 Security Behavioral Intention

Anderson and Agarwal (2010) used the Technology Adoption Model (TAM) (Bagozzi *et al.*, 1992; Davis, 1989) as the foundation for developing their model to study security behavioral intention. The TAM has been extensively used for investigating how the viewpoints of prospective users and users' attitudes and intentions on the new technology affect their technology adoption behavior. The original research of Anderson and Agarwal (2010) has two studies designed for studying the drivers of intentions to perform security-related behavior and their drivers. The first study (see Figure 1) was survey-based research, and the second study was an experiment. In this replication study, we only replicated the survey study. Study 1 of Anderson and Agarwal (2010) investigated their first two research questions, which tried to find the factors influencing a home computer user's security behavior and examined whether there are differences in the factors influencing the protection behavior when the user used a computer versus the Internet. In their study, they collected data from 594 home computer user participants to test their model. They showed that a combination of cognitive, social, and psychological components influenced a user's intention to perform security-related behavior. They also showed that subjective norm and other psychological factors also influenced a user's security-related behavior.

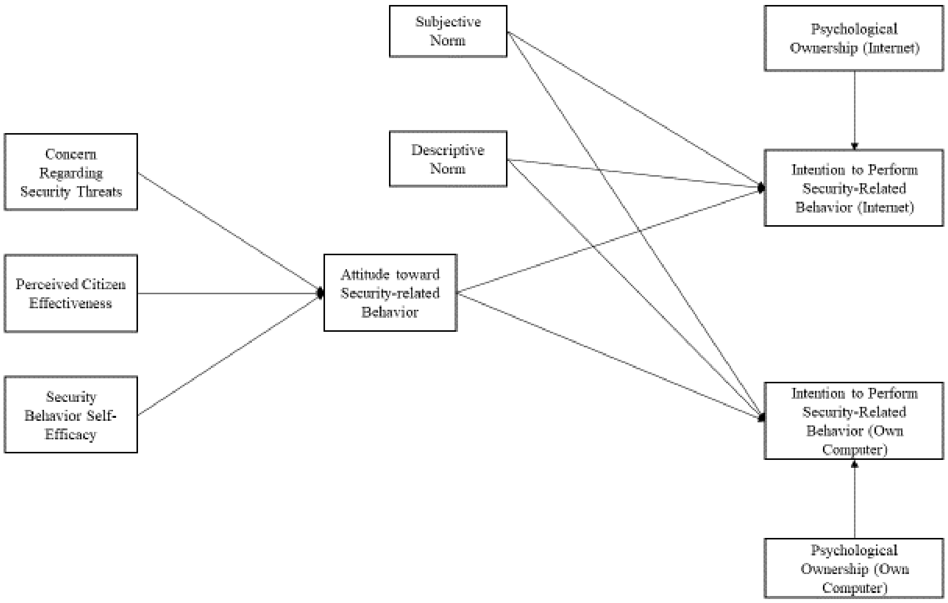
Subjective Norm
Psychological Ownership (Internet)
Concern Regarding Security Threats
Descriptive Norm
Intention to Perform Security-Related Behavior (Internet)
Perceived Citizen Effectiveness
Attitude toward Security-related Behavior
Security Behavior Self-Efficacy
Intention to Perform Security-Related Behavior (Own Computer)
Psychological Ownership (Own Computer)

Figure 1. Research Model Developed by Anderson and Agarwal (2010)

In their study, Anderson and Agarwal (2010) included the following main variables in their model.

Table 1. Main variables used in Anderson and Agarwal (2010)

Main Variable	Description
Subjective norm (SN)	It is the influence of others on the user's decision to use or not to use the technology (Marangunić and Granić, 2015), which has been included in the extended model (TAM2) (Venkatesh and Davis, 2000).
Descriptive norm (DN)	It is related to what an individual believes most other people do. In the information security (InfoSec) context, it is about individuals' expectations of others' InfoSec behavior (Anderson and Agarwal, 2010).
Self-efficacy (SE)	Self-efficacy refers to one's belief about one's ability and competence. Bandura (1989) synthesizes it into the social cognitive theory.
Psychological ownership (PO)	It refers to a state in which a person feels as though the target is "theirs" (Pierce, Kostova, and Dirks, 2003), which is generated from a combination of biological needs and social experiences (Dittmar, 1992; Pierce, Kostova and Dirks, 2003).
Concern regarding security threats (CONC)	It is about the concern on technical guarantees of the systems or technologies involving legal requirements and good practices, including technical, administrative, and managerial controls, related to privacy (Casalo, Flavián, and Guinalíu, 2007; Jennex and Zyngier, 2007).
Intention to Perform Security-related Behavior (INT)	Anderson and Agarwal (2010) suggest that the intention to perform the security-related behavior to protect the Internet and computers owned by the users is positively affected by the user's attitude toward the security-related behavior, as well as DN and SN.

The behavioral intention related to the adoption of technology has been studied extensively in the past few decades. Some research has investigated how culture affects behavioral intention (e.g., Straub *et al.*, 1997). More recently, Ho (2012) conducted a study on the impact of culture on technology adoption, one on the mobile service adoption through comparing data collected from Hong Kong and Guam, and another one on the adoption of environmentally friendly lifestyle through analyzing data collected on Guam and compared with the earlier findings from Japan of Ho and So (2017). These two studies found that the interactions between the TAM constructs are different from location to location, and new relationships are found through a further exploratory study. Therefore, there is a need for IS researchers to investigate further the formation of security behavioral intention under the influence of different locations and among people with different cultural backgrounds.

2.2 Hofstede's Cultural Dimensions

In this study, we collected data from Guam and compared the results reported by Anderson and Agarwal (2010) from US participants. Even though Guam is currently a US unincorporated territory, its culture is different from the US, as reflected by their values of Hofstede's Cultural Dimensions collected from a multinational survey and ranged from a national score of 0 to 100 (Hofstede, 2001; see Table 2). About one-third of Guam's population is Chamorro (the indigenous Pacific Islanders), and another quarter of the population are Filipinos and their descendants. Particularly, Guamanians have a lower level of *power distance* and *masculinity* compared with Americans.

Apart from replicating the study on Guam, we also extended our study to investigate the impact of gender on the model. It is because prior research in TAM (Venkatash and Morris, 2000) reported that gender has a significant impact on a person's technology adoption behavior.

Table 2. Hofstede's Cultural Dimensions

Cultural Dimensions	Definition (Hofstede, 2001)	National Score	
		US	Guam
Power distance	The extent to which the less powerful members of the institutes and organizations with a country expect and accept that power is distributed unequally (p. 98).	40	11
Individualism	It refers to a society in which the ties between individuals are loose (p. 225).	91	86.5
Masculinity	It refers to a society in which social gender roles are clearly distinct (p. 207).	62	25.9
Uncertainty avoidance	The extent to which the members of a culture feel avoidance threatened by uncertainty or an unknown situation (p. 161).	46	55.4
Long-term orientation	It stands for the fostering of virtue orientation towards future rewards, in particular, perseverance and thrift (p. 359).	26	39.8

Note: Hofstede's Cultural Dimension Scores are developed based on Hofstede's multinational survey study (2001). The national score of each dimension is ranked from 0 to 100. The US scores are obtained from https://geerthofstede.com/research-and-vsm/dimension-data-matrix/, and the scores for Guam are obtained from a replicated study by Perez *et al*. (2015).

3 Methodology and Data Collection

As a methodological replicated study, we adopted the survey instrument developed by Anderson and Agarwal (2010) in this study. A priori sample size calculations using an online calculator, as suggested by Westland (2010) (https://www.danielsoper.com/statcalc/calculator.aspx?id=89), and G*Power (Faul *et al.* 2007) had been used to ensure sufficient sample size. We noted that Anderson and Agarwal (2010) only reported the post-hoc statistical power (0.95) but not the effect size. Therefore, we estimated our sample size required using the following parameters, i.e., a medium effect size, statistical power level: 0.9, and probability level: 0.05. Using the design of the original study by Anderson and Agarwal (2010) with ten latent variables and 38 observed variables, we found that the recommended minimum sample size should be around 232 (online calculator) and 250 (G*Power). Thus, we targeted to recruit around 300 participants to join this study.

For the data collection, we invited college students from a local university who enrolled in the undergraduate and graduate business courses to participate in the survey, with extra credit provided as an incentive. Eventually, 322 individuals were recruited to participate in the survey, and their demographics are presented in Table 3. We did not observe any effect of gender on the demographics (all $p > 0.05$).

Table 3. Demographics

	Male (N = 125)	Female (N = 197)	Total (N = 322)
Age	23.3	22.7	22.9
Education (Years counted from elementary school)	15.1	151	15.1
Average Household Income (US$)	$51,580	$45,019	$47,566
Internet Experience (Years)	11.6	10.7	11.1
Frequency of being affected by security violation (1 = infrequently, 7 = frequently)	2.64	2.66	2.65
Heard or read during the last year about security violation (1 = infrequently, 7 = frequently)	4.68	4.94	4.84

4 Data Analysis

We followed Anderson and Agarwal (2010) and used PLS to estimate the full model. In our study, we used Smart PLS 2.0 M3 (Ringle, Wende, and Will, 2005) to perform the PLS analysis. The outer loadings of the PLS result and the correlation matrix are presented in Appendices A and B, respectively. In this study, we noted that the *perceived citizen effectiveness* scale did not converge well. Therefore, we decided to split it into two constructs, i.e., *perceived citizen effectiveness* for the two items with positive coding and *perceived citizen effectiveness (reverse)* for the two reverse-code items. We also confirmed both convergent validities as all t-values of the factor loadings are significant with $p < 0.01$ and all the Cronbach's α values > 0.70 except for *perceived citizen effectiveness*. For *perceived citizen effectiveness*, as its $\alpha = 0.69$ and composite reliability = 0.86, we still considered its convergent validity is achieved. The discriminant validity is also achieved as all instrument items, except SE4 and SE5, have a loading > 0.7 on their associated factors and have a low loading on other factors (Nunnally, 1978). Also, the square root of the average variance extracted of each latent construct in Appendix B. As the revised model had 11 constructs, we recalculated the minimum sample size of our model. The minimum sample size should be between 238 (online calculator) and 250 (G*Power). Therefore, our sample size (n = 322) was sufficient for conducting our data analysis.

The descriptive statistics of our constructs, which are presented in Table 4, with a further breakdown based on gender and compared with the results reported by Anderson and Agarwal (2010). We noted the effect of gender on the following constructs: *concerns* (female [mean = 6.20] > male [mean = 5.94], p = 0.02), *perceived citizen effectiveness (reverse)* (female [mean = 5.03] > male [mean = 4.46], p < 0.01), *psychological ownership for own computer* (male [mean = 6.04] > female [mean = 5.69], p = 0.02), *security behavioral intention (own computer)* (male [mean = 6.04] > female [mean = 5.74], p = 0.02), and *security behavioral intention (Internet)* (male [mean = 5.67] > female [mean = 5.34], p = 0.02).

We also compared the mean values of the constructs found in our dataset with the original study using *t*-tests. The results showed statistically significant differences in the mean values. The values of *concern*, *perceived citizen effectiveness*, *subjective norm*, and *psychological ownership for Internet* of data collected from Guam are statistically higher than those collected from Anderson and Agarwal (2010). In contrast, *self-efficacy*, *psychological ownership for own computer*, and *security behavioral intention of own computer* are lower than Anderson and Agarwal's (2010) values.

Table 4. Descriptive Statistics

Construct	**Replication Study**					**Original**	**Difference**
	α	**CR**	**Male**	**Female**	**Total**		
Concern (CONC)	0.92	0.94	5.94	6.20	6.10	5.17	0.93 ***
Perceived citizen effectiveness (PCE)	0.69	0.86	5.68	5.76	5.73	4.86	0.56 ***
Perceived citizen effectiveness – Reverse (PCE(R))	0.80	0.91	4.46	5.03	4.81	4.86	–0.05
Self-efficacy (SE)	0.86	0.87	4.76	4.76	4.76	5.10	–0.34 ***
Security behavioral attitude (ATT)	0.93	0.96	6.41	6.41	6.41	6.35	0.06
Subjective norm (SN)	0.89	0.93	4.98	5.06	5.03	4.73	0.30 **
Descriptive norm (DN)	0.89	0.92	4.61	4.57	4.59	4.74	–0.15
Psychological ownership for own computer (POC)	0.93	0.96	6.04	5.69	5.83	6.20	–0.37 ***
Psychological ownership for Internet (POI)	0.83	0.90	3.85	3.62	3.71	3.44	0.27 *
Security behavioral intention (own computer) (INTC)	0.94	0.96	6.04	5.74	5.86	6.16	–0.30 ***
Security behavioral intention (Internet) (INTI)	0.94	0.96	5.67	5.34	5.47	5.50	0.03

Notes: *** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$; α = Cronbach's alpha; CR = Composite reliability. The "Difference" reported the differences between the mean values of the total value of the replication study with the original study. For example, for "Concern," the difference, 0.93, is calculated by the value of the mean value of "Replication Study" (6.10) subtracting "Original" (5.17). We also tested whether the value of "Difference" is statistically significant by t-tests.

The results are summarized in Table 5. Our model is slightly different from those of Anderson and Agarwal (2010). As mentioned above, we separated *perceived citizen effectiveness* into two constructs, i.e., *perceived citizen effectiveness* and *perceived citizen effectiveness (reverse)*. There were four significant differences between our model and Anderson and Agarwal's model. First, we needed to split *perceived citizen effectiveness* into two constructs, and both constructs have significant positive impacts on security behavioral attitude (i.e., H2a and H2b). Second, we observed a significant impact of the *descriptive norm* on *security behavioral intention (own computer)*, which the prior study did not observe. Third, we also observed the significant impact of the *subjective norm* on *security behavioral intention (Internet)*, which the prior study did not observe. Last, we did not observe the impact of the *descriptive norm* on *security behavioral intention (Internet)*.

Table 5. Results

Hypothesis	Replication Study		Original	
	Coefficient	Support?	Coefficient	Support?
Security behavioral attitude (ATT)	$R^2 = 0.24$		R^2 not reported	
H1: CONC → ATT	0.21^{**}	Yes	0.36^{**}	Yes
H2: PCE → ATT	N/A		0.15^{**}	Yes
H2a: PCE → ATT	0.20^{**}	Yes	N/A	
H2b: PCE(R) → ATT	0.24^{***}	Yes	N/A	
H3: SE → ATT	0.16^{**}	Yes	0.32^{**}	Yes
Security behavioral intention (own computer) (INTC)	$R^2 = 0.40$		$R^2 = 0.43$	
H4b: Attitude → INTC	0.45^{***}	Yes	0.61^{***}	Yes
H5b: SN → INTC	0.21^{***}	Yes	0.12^{*}	Yes
H6b: DN → INTC	0.16^{**}	Yes	0.04	No
H7b: POC → INTC	0.13^{*}	Yes	0.05^{*}	Yes
Security behavioral intention (Internet) (INTI)	$R^2 = 0.46$		$R^2 = 0.35$	
H4a: Attitude → INTI	0.11^{*}	Yes	0.15^{**}	Yes
H5a: SN → INTI	0.15^{*}	Yes	–0.01	No
H6a: DN → INTI	–0.01	No	0.08^{*}	Yes
H7a: POI → INTI	0.20^{***}	Yes	0.16^{***}	Yes
Control: INTI → INTI	0.48^{***}	Yes	Not reported	

Notes: *** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$. The following control was significant and included in the model: gender has a positive impact on INTI.

5 Discussion

Using student participants recruited from Guam, the findings of this study are very similar to those reported by Anderson and Agarwal (2010). However, there are still some new findings in this replication study.

5.1 Effect of Gender

First, apart from replicating the previous study, we also explored gender effect on the constructs. Prior research, for example, Anwar *et al*. (2017), has pointed out that gender types had effects on information security behavior. In this study, we also observed gender effects on some of the constructs, such as *information security concerns*, *perceived citizen effectiveness (reverse)*, *psychological ownership for own computer*, *security behavioral intention (own computer)*, and *security behavioral intention (Internet)*. This finding suggested that when practitioners would like to design mechanisms to encourage practicing information security behavior, they should consider gender as users of a different gender would have different security concerns and have different security behaviors.

5.2 Possible Effect of Individualism and Power Distance

In this study, we noted that the 4-item construct of *perceived citizen effectiveness* proposed by Anderson and Agarwal (2010) did not converge. In the original study, Anderson and Agarwal (2010) already reported that even the four items converged into a construct, the positive and reverse code did not converge well. In this study, as reported earlier, these four items could not converge well into a construct, and we decided to split it into two separate constructs. Prior research (van Sonderen, Sanderman and Coyne, 2013; Weijters, Baumgartner and Schillewaert, 2013) suggested that the non-convergent of constructs with both positive and reverse items might be due to the misunderstanding of the respondents. We are of the view that there is another possible explanation for this case.

From the correlation matrix in Appendix A, we noted that the two constructs correlated with the other constructs in the model differently. Also, the two reverse coded items are indicating the lack of a person's ability to contribute to the Internet (i.e., the collective group of users of Internet), i.e., "*the efforts of one* *person are useless in helping secure the Internet*,” and “*there is not much that any one individual can do to help secure the Internet*.” However, as both the United States and Guam are locations with high *individualism*, the loose ties between individuals within society may reduce the trust of others. Thus, our respondents might think negatively about the ability of an individual to contribute to collaborative work (Kiffin-Petersen and Cordery, 2003), such as the protection of the Internet. Therefore, we recommend conducting further research using data collected from countries with high *collectivism* (i.e., low *individualism* scores, such as Hong Kong, score = 25 and Japan = 46). These future research studies can help verify if the non-convergent effect of a misunderstanding of the scale or cultural issue exists.

The other significant differences are the impacts of the *descriptive norm* and *subjective norm* to the *security behavior intentions* (both to the computer and the Internet) are different in these two studies. For the original study, the *subjective norm* impacts *security behavior intentions (own computer)*, and the *descriptive norm* impacts *security behavior intentions (own Internet)*. However, for this study, we note that *subjective norm* impacts both *security behavior intentions (own computer)* and *security behavior intentions (own Internet)*, and *descriptive norm* has an impact on *security behavior intentions (own computer)* only.

In this study, the *subjective norm* is defined as how others influence the user to perform InfoSec behavior. Prior research has mixed results regarding how culture, and in particular, *individualism*, affects *subjective norm*. Some studies suggested the impact of *subjective norm* on intention only existed in collectivist culture (i.e., with low individualism score) (Lee and Wan, 2010; Schepers and Wetzels, 2007), while others reported suggested that such effect also exists in individualism culture (Yang and Jolly, 2009).

In this study and the original study, we observed the significant effect of *subjective norm* on *security behavior intentions (own computer)*, and a similar effect is only observed on *security behavior intentions (own Internet)* for data collected from Guam. These results supported more on the argument that the impact of the *subjective norm* would exist in an individualist culture. In this research context, the *subjective norm* is how others influence the user’s intention to take security behavior. It is because such behavior is personal behavior, and it is their responsibility to protect their computers. Therefore, we observe the positive result for the *subjective norm* influencing *security behavior intentions (own computer)* and *security behavior intentions (own Internet)*.

For the *descriptive norm*, prior research has suggested that *power distance* would impact it (Gelfand and Harrington, 2015). As mentioned, in this research context, the *descriptive norm* is the expectation of others on performing InfoSec behavior. Comparing the United States and Guam, Guam’s culture has a low *power distance*. Therefore, the *descriptive norm* may significantly impact *security behavior intentions (own Internet)* for the United States. It is because the United States has a more substantial influence on *power distance* and would encourage participants to follow the *descriptive norm* to take up their responsibility to adopt a more active role in taking up security behavior intentions. As the responsibility taken by other people would be more observable for the Internet (as their computers are connected) and thus, the effect would be more significant for the Internet. The comparative findings also show this effect, i.e., *descriptive norm* only impacts the *security behavior intentions (own Internet)* for the United States, but not for Guam.

6 Concluding Remarks

This study is a methodological replication study using the model developed by Anderson and Agarwal (2010) for studying the formation of information security behavioral intention. Replication study is typical in physical science research to confirm findings, yet it is rare to conduct replication study in IS research until recently (Dennis and Valacich, 2015).

The finding of this study generally supports the Anderson and Agarwal (2010) model despite the demographic (i.e., Anderson and Agarwal (2010) were using the general public, and our study was using student participants) and time differences (i.e., the two studies were conducted ten years apart). Therefore, we can argue that the Anderson and Agarwal (2010) model is generalizable to the population on Guam. We also noted that we provided incentives (extra credits) to invite our students to participate in the survey. In contrast, the original study did not report whether they provided incentives to recruit their participants. While we did not directly measure the cultural difference between the two samples, we note that the participants’ cultural backgrounds may explain the differences in the findings. Therefore, we would recommend conducting more replication studies to examine how culture would affect our security behavior intention.

References

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613-643.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437-443.

Bagozzi, R. P., Davis, F. D., & Warshaw, P. R. (1992). Development and test of a theory of technological learning and usage. *Human Relations*, 45(7), 659-686.

Bandura, A. (1989). Social cognitive theory. In *Annals of Child Development*, Volume 6, (pp. 1-60). Greenwich, CT: JAI Press.

Casalo, L. V., Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review*, 31(5), 583-603.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-340.

Dennis, A. R., & Valacich, J. S. (2015). A replication manifesto. *AIS Transactions on Replication Research*, 1(1), 1-4.

Dittmar, H. (1992). *The Social Psychology of Material Possessions: To Have is to Be*, New York, NY: St. Martin's Press.

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, 39, 175-191.

Gelfand, M. J., & Harrington, J. R. (2015). The motivational force of descriptive norms: For whom and when are descriptive norms most predictive of behavior? *Journal of Cross-Cultural Psychology*, 46(10), 1273-1278.

Ho, K. K. W. (2012). A study on the intention to adopt third generation (3G) wireless service on a small community with unique culture: The use of Hofstede Cultural Dimensions in predicting the interaction between culture and the technology acceptance model on Guam. *International Journal of Systems and Service-Oriented Engineering*, 3(4), 57-77.

Ho, K. K. W., & So, S. (2017). Towards a smart city through household recycling and waste management: A study on the factors affecting environmental friendliness lifestyle of Guamanian. *International Journal of Sustainable Real Estate and Construction Economics*, 1(1), 89-108.

Hofstede, G. H. (2001). *Culture's Consequences: Comparing Values, Behaviors, Institutes, and Organizations across Nations*, 2nd ed., Thousand Oaks, CA: Sage Publications, Inc.

Im, G., & Straub, D. (2015). The critical role of external validity in advancing organizational theorizing. *Communications of the Association for Information Systems*, 37(1), Article 44.

Jennex, M. E., & Zyngier, S. (2007). Security as a contributor to knowledge management success. *Information Systems Frontiers*, 9(5), 493-504.

Kiffin-Petersen, S. A., & Cordery J. L. (2003). Trust, individualism and job characteristics as predictors of employee preference for teamwork. *International Journal of Human Resources Management*, 14(1), 93-116.

Lee, C. B. P., & Wan, G. (2010). Including subjective norm and technology trust in the technology acceptance model: A case of e-ticketing in China. *The DATA BASE for Advances in Information Systems*, 41(4), 40-51.

Marangunić, N., & Granić, A. (2015). Technology acceptance model: A literature review from 1986 to 2013. *Universal Access in the Information Society*, 14(1), 81-95.

Nunnally, J. C. (1978). *Psychometric Theory*. 2nd Edition. New York, NY: McGraw-Hill.

Perez, K., Dote, K., Damian, J., Taylor, M., & Dickens, A. (2015). *Guam and Saipan's business culture: Deriving Hofstede's score*. Mangilao, GU: Pacific Center for Economic Initiatives, University of Guam.

Pierce, J., Kostova, T., & Dirks, K. T. (2003). The state of psychological ownership: Integrating and extending a century of research. *Review of General Psychology*, 7(1), 84-107.

Ringle, C. M., Wende, S., & Will, A. (2005). SmartPLS 2.0.M3. Hamburg: SmartPLS, http://www.smartpls.de

Schepers, J., & Wetzels, M. (2007). A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects. *Information & Management*, 40(1), 90-103.

Straub, D., Keil, M., & Brenner, W. (1997). Testing the technology acceptance model across cultures: A three country study. *Information & Management*, 33(1), 1-11.

Van Sonderen, E., Sanderman, R., & Coyne, J. C. (2013). Ineffectiveness of reverse wording of questionnaire items: Let's learn from cows in the rain. *PLoS ONE*, 8(7), e68967.

Weijters, B., Baumgartner, H., & Schillewaert, N. (2013). Reversed item bias: An integrative model. *Psychological Methods*, 18(3), 320-334.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186-204.

Venkatesh, V., & Morris, M. G. (2000). Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS Quarterly*, 24(1), 115-139.

Westland, C. J. (2010). Lower bounds on sample size in structural equation modeling. *Electronic Commerce Research and Applications*, 9(6), 476-487.

Yang, K., & Jolly, L. D. (2009). The effects of consumer perceived value and subjective norm on mobile data service adoption between American and Korean Consumers. *Journal of Retailing and Consumer Services*, 16(6), 502-508.

Appendix A: Outer Loadings of PLS Models

Items	CONC	PCE	PCE(R)	SE	ATT	SN	DN	POC	POI	INTC	INTI
CONC1	0.69										
CONC2	0.79										
CONC3	0.83										
CONC4	0.87										
CONC5	0.86										
CONC6	0.80										
CONC7	0.79										
CONC8	0.81										
PCE1		0.81									
PCE3		0.92									
PCE2(R)			0.91								
PCE4(R)			0.92								
SE1				0.93							
SE2				0.93							
SE3				0.78							
SE4				0.58							
SE5				0.50							
ATT1					0.93						
ATT2					0.95						
ATT3					0.93						
SN1						0.91					
SN2						0.90					
SN3						0.92					
DN1							0.87				
DN2							0.87				
DN3							0.90				
DN4							0.82				
POC1								0.93			
POC2								0.95			
POC3								0.92			
POI1									0.80		
POI2									0.94		
POI3									0.85		
INTC1										0.94	
INTC2										0.94	
INTC3										0.95	
INTI1											0.95
INTI2											0.94
INTI3											0.96

Notes:
CONC = Concern; PCE = Perceived citizen effectiveness (PCE); PCE(R) = Perceived citizen effectiveness (Reverse Code); SE = Self-efficacy; ATT = Security behavioral attitude; SN = Subjective norm; DN = Descriptive norm; POC = Psychological ownership for own computer; POI: Psychological ownership for Internet; INTC = Security behavioral intention (Own computer); and INTI = Security behavioral intention (Internet)

Appendix B: Correlation Matrix

Items	√AVE		CONC	PCE	PCE(R)	SE	ATT	SN	DN	POC	POI	INTC	INTI
	Replication Study	Original											
CONC	0.81	Not reported		0.27		0.13	0.46	0.17	0.19	0.19	0.09	0.31	0.27
PCE	0.87	0.79	0.28			0.32	0.36	0.11	0.14	0.18	0.15	0.31	0.51
PCE(R)	0.96	-	0.07	0.17									
SE	0.77	0.86	0.18	0.31	–0.08		0.41	0.09	0.19	0.12	0.11	0.44	0.38
ATT	0.94	0.91	0.31	0.35	0.27	0.24		0.13	0.18	0.21	–0.02	0.64	0.43
SN	0.91	0.93	0.20	0.32	–0.21	0.35	0.15		0.21	0.12	0.11	0.44	0.38
DN	0.86	0.87	0.13	0.27	–0.27	0.31	0.03	0.43		0.03	0.23	0.18	0.23
POC	0.94	0.95	0.12	0.24	0.08	0.17	0.40	0.13	0.12		0.17	0.19	0.11
POI	0.87	0.95	0.03	0.18	–0.23	0.13	0.04	0.18	0.30	0.22		0.01	0.21
INTC	0.94	0.90	0.23	0.30	0.05	0.31	0.54	0.36	0.27	0.36	0.16		0.52
INTI	0.95	0.94	0.20	0.34	0.02	0.29	0.40	0.37	0.25	0.22	0.30	0.63	

Notes:
AVE = Average variance extracted.
Correlation of original study in the upper right half of the matrix, and replication study in the lower left half of the matrix.
CONC = Concern; PCE = Perceived citizen effectiveness (PCE); PCE(R) = Perceived citizen effectiveness (Reverse Code); SE = Self-efficacy; ATT = Security behavioral attitude; SN = Subjective norm; DN = Descriptive norm; POC = Psychological ownership for own computer; POI: Psychological ownership for Internet; INTC = Security behavioral intention (Own computer); and INTI = Security behavioral intention (Internet)

About the Authors

Kevin K.W. Ho is a Professor at the School of Business and Public Administration, University of Guam. Kevin's research interests include electronic service, information systems strategy, social media, green information systems, sustainability management, and electronic government. He is currently the Co-Editor(-in-Chief) of *Library Hi Tech* and an associate editor in *International Journal of Systems and Service-Oriented Engineering*. His research has been published in *Australian Journal of Management*, *Behaviour & IT*, *Communications of the Association for Information Systems*, *Computers in Human Behavior*, *Decision Support Systems*, *Health Policy*, *Information & Management*, *Information Systems Frontier*, *Internet Research*, *Journal of Electronic Commerce Research*, *Online Information Review*, among others.

Cheuk Hang (Allen) Au is an Assistant Professor from the Department of Information Management at the National Chung Cheng University. His research focuses on digital entrepreneurship and computer-mediated communications. His publications can be found in a number of journals such as *Communications of the Association for Information Systems*, *Internet Research*, *Australian Journal of Management*, and the *Journal of Computer Information Systems*.

Dickson K.W. Chiu is a faculty member at the University of Hong Kong. His teaching and research interests are in Information Management, Service Computing, Library Science, and E-learning with a cross-disciplinary approach, involving workflows, software engineering, information technologies, agents, information system research, and databases. The results have been widely published in over 250 international publications (most of them indexed by SCI, SCI-E, EI, and SSCI), including many practical taught master and undergraduate project results. He received a best paper award in the 37th Hawaii International Conference on System Sciences in 2004. He is the founding Editor-in-chief of the *International Journal on Systems and Service-Oriented Engineering*, and serves on the editorial boards of several international journals. He is an editor(-in-chief) of *Library Hi Tech*, and a Senior Member of both the ACM and the IEEE, and a life member of the Hong Kong Computer Society.