Academia Journal of Educational Research 3(3): 000-000, April 2020
DOI: 10.15413/ajer.2020.0113
ISSN 2315-7704
©2020 Academia Publishing

Academia Publishing

Research Paper

The effect of uncertainty avoidance on behavioral information security

Accepted 14th April, 2020

Xiaojuan Zhang[1], Xinluan Tian[2] and Hui Yang[3]*

[1]School of Information Management, Wuhan University, No. 299, Bayi Road, Wuchang District, Wuhan City, Hubei Province, 430072, China.
[2]School of Information Management, Wuhan University, No. 299, Bayi Road, Wuchang District, Wuhan City, Hubei Province, 430072, China.
[3]Library of National Defence University, Haidian District, Beijing City, 100091, China.

*Correspondence author. E-mail: YHYH2018@yeah.net. Tel: +86 15890921010.

ABSTRACT

It is commonly considered that culture has an influence on individuals' information behaviors, and specifically the degree of uncertainty avoidance (UA) in different cultures is one of the important factors to information security behaviors. However, the pattern of UA's impact on information security behavior remains unknown. In this study, the Theory of Planned Behavior (TPB) is introduced to construct a model of uncertainty avoidance's influence on information security behavior, followed by a cross-cultural empirical study on 229 university students from various country. The results show that UA has a significant impact on the intention for individuals with different cultural backgrounds to take part in information security behaviors. However, the impact is not directly, but indirectly generated through behavioral attitude, subjective norm, and perceived behavioral control. To the best of our knowledge, this study is the first to introduce the TPB into the exploration of the impact of UI on information security behaviors, through which the authors determine the pattern of the impact. This research could be of help not only for rightfully handling dissimilarities in individuals' behaviors but also for policy makers to formulate workable policies based on different culture.

Key words: Cross cultural comparison, information security, behavioral information security, Hofstede cultural dimensions, uncertainty avoidance.

INTRODUCTION

Openness of information systems by itself makes it unavoidable that their developments and usages will be threatened by multiple factors, such as intentional human damage, physical malfunction, etc. As the degree of global informatization continue to rise, instances of user information security behaviors increase sharply. Varieties of these behaviors are also becoming heterogeneous. Information security risks likewise go up correspondingly. Examples include leaks of individual or enterprise information (Zafar and Clark, 2009), stolen personal information (Parsons et al., 2014), and malware attacks (Solms and Niekerk, 2013). These issues will lead to disclosure of important information of personal users, governments or enterprises, which may result in huge losses. Therefore, people will make efforts to lower the information security risks through security means, e.g., encrypting important information (Puhakainen and Siponen, 2010), backing up data (Lebek et al., 2014), installing anti-virus software or firewall for computers (Safa et al., 2015), and setting log in password for electronic devices (Puhakainen and Siponen, 2010; Samhan, 2017), etc.

The technical solutions are necessary but not sufficient to provide full security protection for computer systems. Academic research in information security related fields has revealed that information security risks caused by technical problems are gradually getting lower (Dhillon et al., 2016), and that currently the greater information security risks are posed by various weaknesses, errors and habits of information behaviors of users (Crossler et al., 2013). Hence, it also depends on people's effective information security behavior to manage information security risks (Rhodes, 2001; Crossler et al., 2013).

In addition, it is observed that individuals evaluate and accept negative risks in different ways, which will affect the decisions associated with individual information security

behaviors. Voluntary information security behaviors generally require an assessment of the risks, then a decision would be made on basis (Posey et al., 2015). In theory, the assessment would affect the individual's adoption of security measures (Albrechtsen, 2007; Straub and Welke, 1998). For instance, when deciding to use a password manager application, individuals have evaluated the likelihood and consequences of a stray password. The level of assessment of uncertainty risk will increase or decrease an individual's motivation to adopt the information security control voluntarily. It is interesting to note that socialization in different national cultures would result in different levels of tolerance for risk and uncertainty, termed uncertainty avoidance(UA) (Hofstede, 2001). For example, people in Singapore, Jamaica and Denmark have lower uncertainty in social activities, while people in countries such as Greece and Portugal are more inclined to avoid risks (Aurigemma and Mattson, 2018). Given the importance of assessing risk and uncertainty in voluntary information security decisions, it can be hypothesized that individuals socialized in different national cultures will have varying tolerances of uncertainty and thus take different information security behavior. Most researchers in information security area consider the UA dimension to be the most influential cultural dimension for explaining various technology related phenomena (Cardon, 2008; Straub and Hill, 2002, Aurigemma and Mattson, 2018). However, no scholars have paid attention to the pattern on which uncertainty avoidance affects information security behavior. Hence in this study, we make our efforts to address the following research question:

RQ: Does avoidance uncertainty have an impact on information security behavior, and if so, in what pattern?

THEORETICAL FOUNDATIONS

Culture

Culture is commonly considered to be one of the main propellants behind human behaviors (Hofstede, 1993). However, scholars conducted a variety of debates on the definition of culture in existing related literatures. In this study, we adopted "the collective programming of the mind which distinguishes one group from the other" as the concept of culture. It can be interpreted that culture is the way of processing information and understanding the world of social members, including different social, political, educational, communal and economic means (Hofstede, 1993). Via this logic, social members with common value system and norms formed cultural body, through which individuals decide which behaviors are suitable or not in a particular situation (Tierney and Schein, 1986).

Culture plays an important role in determining how individuals and groups express and think (Crossler et al., 2013; Wang et al., 2017). Dissimilar cultures have varying thought patterns and values along many dimensions, providing a framework for individuals to use in their daily decision-making processes. Cultural theorists have determined that national cultures differ on many characteristics and dimensions. For example, Trompenaars and Hampden-Turner (2011), as well as House et al. (2004), discussed about ethnic cultural differences that involved interpersonal communication, time orientation, and spatial perception. In the field of information systems, Hofstede model is the most commonly used in national culture issues, which consists of six dimensions, which are Power Distance, Individualism vs Collectivism, Uncertainty Avoidance, Long-term Orientation vs Short-term Orientation, Indulgence vs Restraint, and Masculinity vs Femininity. It is worthy of note that Hofstede's theory of cultural dimensions has been employed to analyze issues related to information security (Dinev et al., 2009; Lowry et al., 2011). In both multiple information behavior scenarios, such as personal online socializing and knowledge sharing (Choi and Hofstede, 2016; Zhang et al., 2014), and information systems usage behaviors of organisational staff and e-commerce transaction behaviors (Mohammed and Tejay, 2017; D'Arcy et al., 2009), cultural differences have proven to be a significant factor that influences information security related behaviors.

Recently, studies on behavioral information security were conducted to investigate how cultural differences at national level affect security related actions (Dinev et al., 2009; Hovav and D'Arcy, 2012; Lowry et al., 2014). Existing research indicates that national culture is an important factor behind individuals' information security acts. For instance, Hovav and D'Arcy (2012) explored how national culture affect employee information system misuse intentions. They showed that behavioral theories developed and tested in Western cultures may work differently in other cultures. The researchers argued that different information security behaviors should surface from individuals with different national culture backgrounds. Therefore, for the best education and conscientization of security stakeholders, further evaluation of the effect of national culture on information security behaviors is needed (Karjalainen et al., 2013).

The cultural dimension of UA was developed specifically to address cross-cultural differences regarding uncertainty when making decisions (Hofstede, 2001). Uncertainty avoidance describes the degree of acceptance towards unknown or uncertain matters for individuals in society. Individuals with high UA would be more prudent when bearing risks and accepting uncertainty, and simultaneously intense anxiety is shown. On the other hand, facing the same situation individuals with low UA will be calmer, which shows they have a higher acceptance towards the unknown (Hofstede et al., 2010). As an illustration, staff from cultural backgrounds with lower UA

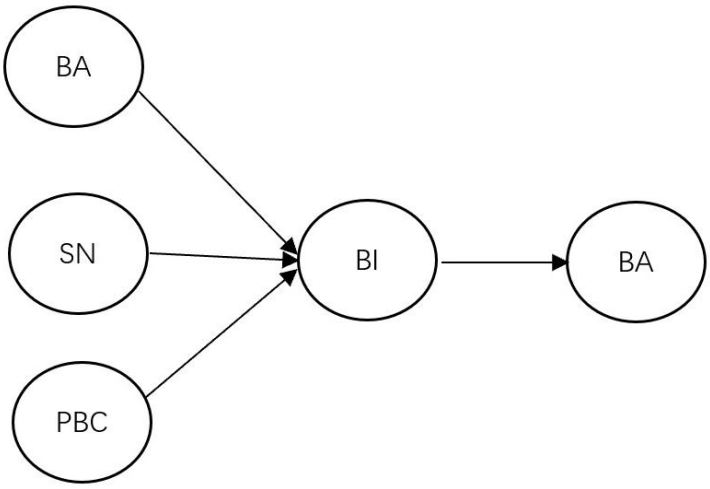

Figure 1: TPB (Theory of Planned Behavior) model.
BA = Behavior Attitude, BI = Behavioral Intention, BE = Behavior.

will display a relaxed attitude when facing unknown situations (Aurigemma and Mattson, 2018). For example, there is a higher chance for these staff to open emails from unknown sources (Crossler et al., 2013). This finding has also been confirmed in other studies (Lai et al., 2016; Crossler et al., 2013). However, how UA as a cultural phenomenon affects the decision intention of individuals voluntarily adopting information security behaviors is still not explored in the literature.

Theory of planned behavior

There is no universally accepted "correct" theory that explains the majority of the differences in information security behaviors (Aurigemma and Mattson, 2018). In the past decades, scholars have debated the merits and defects associated with each of these theoretical approaches. In the present study, we chose the theory of planned behavior (TPB), which has been proposed by Ajzen in 1985, to explore individuals' information security behavior. The TPB is a comprehensive theory combined with psychology and behavioral theory to help understand how people change their behavior patterns. TPB believes that human behavior is the result of a sophisticated consideration, which means a person's behaviors would be predicted by the intention, which is determined by attitude (BA), subjective norm (SN) and perceived behavior control (PBC) together.

TPB theory is widely employed in many areas of security research to explore individual information security behaviors in different scenarios. For example, research findings in Kam (2014) suggest that, regulatory and subjective normative pressure indirectly promotes information security in higher education. The research of Chang (2009) shows that for selfie-posting, attitude, subjective norm, perceived behavioral control and narcissism are the significant determinants of an individual's intention to post selfies on social networking sites (SNSs). The research from Kim et al. (2016) indicates the attitude, SN, PBC and narcissism together constitute the determinative role in users disclosing personal information on social networks. The study of Pavlou and Fygenson (2006) extends Ajzen's TPB theory to explain and predict the process of e-commerce adoption by consumers.

However, to the best of our knowledge, although TPB has been successfully used in predicting multiple types of behaviors and understanding the influence on decisions of user information security behaviors, no existing research has investigates the potential roles of national culture, specifically the UA dimension of national culture, in person's security behaviors using any of the TPB models. This omission is significant because individuals socialized in different cultures develop different thought patterns, values, and culturally defined norms (Schein, 2010; Triandis, 1994), which may impact their information behavior including information security behaviors. In addition, TPB is a revised version of theory of rational action (TRA) which is mainly used for a deep understanding the predictive factors for individuals' tendency to make information security decisions. By introducing the TPB into our research, we expect that it will be able to help with the exploration of the influence pattern of UA's on security behavior from the perspective of cross-culture (Figure 1).

CONCEPTUAL MODEL

Behavior attitude and uncertainty avoidance

Attitude is an important variable in the TPB theory. It refers to the integrated evaluation of individuals on all possible

consequences from their behaviors (Ajzen, 1991). Prior et al. (2016) show their findings from an online survey of 151 postgraduate business students. They suggested that positive student attitude significantly contribute to self-efficacy in online distance education. In information security area, the research of Shropshire and Warkentin (2015) points out that individual attitude towards information security behaviors significantly affect users' response efficacy and self-efficacy, further influencing their intention to elicit secure information behaviors. Park's studies (2014, 2017) indicate that in multiple environments, attitude of users towards information security technology can influence their evaluation of whether the technology would be of help in protecting their personal information security. Thus when user's attitudes are more positive, their sense of self-efficacy will be higher, which will finally affect their behavioral intention. This indicates that individuals ' behavior attitude possesses significant positive effect on their behavioral intention.

Based on the above discussed, existing research deduces that when individuals have positive attitude towards information security behaviors, then their intention to adopt information security behaviors will be raised. At the same time, there is also positive influence on their assessment of their own ability to respond to information security risks, thus significantly ascending the intention for information security behaviors. On such bases, we propose a hypothesis as the follow:

H1: Individuals'UA possesses significant positive correlation to behavior attitude.

Subjective norm and uncertainty avoidance

Subjective norm refers to the degree of individuals' feeling on surrounding pressures when they generate information security behaviors and adopt information security measures. These influences include those from family, friends, tutors and superiors, as well as media promotion and exemplars in the social environment they are situated in. Existing studies on information system and information security have already paid attention to the influence of subjective norm on individual behaviors (Schepers and Wetzels, 2015; Cheung et al., 2017). Yoon (2012) confirmed that in a school setting, the higher the degree of subjective norm for students is, the greater the influence of pressure from teachers on them will be. Hence, the extent of intention producing secure behaviors will be greater. In the contexts of company and market, staff's subjective norm has significant influence on behavioral intention and can help the staff establish information behaviors in line with security norms in the end (Schepers et al., 2007; Yazdanmehr and Wang, 2016). In the Internet context, the research of Safa et al. (2015) showed that subjective norms have a positive effect on users' behavior.

Summarizing the background research, our deduction is that the higher the extent of subjective norm for a person, the greater the external pressure will be felt and the individual's intention for information security behaviors will become higher. The lower the external pressure the individuals feels, the lower the intention for information security behaviors will be. On the basis, we hypothesize the following:

H2: UA has a positive influence on subjective norm.

Perceived behavioral control (PBC) and uncertainty avoidance

The factors of perceived behavioral control play an significant role in the theory of planned behavior, because it expands the applicability of the theory to more complex goals and results. A study has shown that perceived behavioral control is the most decisive factor for individual's energy-saving intention (Xing et al., 2018). Perceived behavioral control is an individual's perception of complexity on the behavior. This suggests that people are more likely to engage in controlled behavior, while they are less likely to engage in uncontrolled behavior. For example, an empirical study on healthy lifestyle in Singapore showed that perceived behavioral control was positively correlated with behavioral intention (Banerjee and Ho, 2019). Therefore, when users have a high degree of uncertainty avoidance, they are more cautious in the face of risks and are more willing to participate in controllable behaviors. Hence, we hypothesize:

H3： UA has positive correlation with perceived behavioral control.

Behavioral intention and uncertainty avoidance

Uncertainty avoidance describes how well individuals accept unknown or uncertain things in society. From its definition, people with high uncertainty avoidance are more cautious in taking risks and accepting uncertainty, and show strong uneasiness, while people with low uncertainty avoidance are more peaceful in the face of the same situation, and have higher acceptance of the unknown (Aurigemma and Mattson, 2018). Previous studies have shown that employees with low uncertainty and cultural background are more likely to open e-mails from unknown sources, which will lead to information security risks, such as virus intrusion, phishing attacks, corporate information disclosure, etc. On the contrary, employees with high uncertainty avoidance culture will feel threat and pressure in the face of unknown situation, and try to seek support from their superiors (Crossler et al., 2013). Based on the above discussion, it can be conjectured that for a person

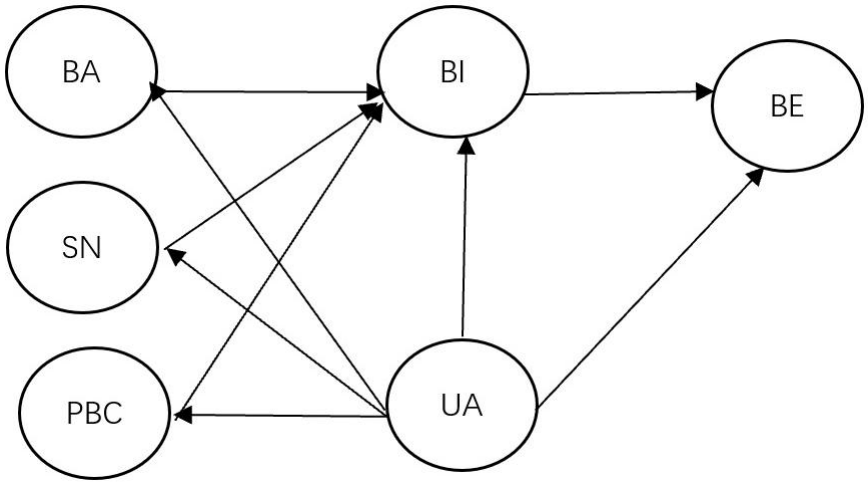

Figure 2: Conceptual model of UA's impact on information security behaviour.

with a higher degree of UA, his/her information security behavioral intention will be higher. Thus we hypothesize:

H4: UA has positive correlation with their behavioral intention

Behavior and uncertainty avoidance

According to the theory of planned behavior, people's behavior can be predicted by their intention. The possibility of a person's behavior is directly proportional to his behavior intention. On the basis of the above hypotheses, it can be conjectured that the higher the degree of UA in a person, the higher his/her intention to carry out the behavior, namely more information security actions from the individual. Thus, it is hypothesized:

H5: In information security behaviors, individuals' UA has positive correlation with behavior.

From the above hypotheses, the study introduces uncertainty avoidance as the cultural variable functioning as the moderator to construct a conceptual model in combination with TPB of influencing factors in UA. In the conceptual model of this study, UA is set as a mediator variable to study if it can impact information behavioral intention and behavioral information security.

CALCULATION

Survey design

The conceptual model in Figure 2 comprises six potential variables. Each of them is composed of observed variables. To ensure the content validity of the observed variables, we adapted measurement items according to university students' characteristics for our constructs from reflective scales taken from previous UA compliance and national culture research.

The measurement items are shown in Table 1. A seven-point Likert scale is used to obtain respondents' assessments of a range of information security compliance items, with "7" denoting 'highly important' and "1" representing 'not important at all'.

Data collection

To study the influence of UA on individual security information behavior in different culture, we compared participants from multiple countries, including mainland China, Canada, and USA. Our sample comprised university students since they are active users and communicators of network information. Multiple studies indicate that university students' web usage is alarmingly high (Junco, 2011).

The network survey of information behaviors was done online. The instrument of this study was distributed to university students in China, USA, Canada and other countries. To ensure the validity and structural logicality of the questionnaire when its design was first completed, the questionnaire was tested by experts in the field of information security and information systems.

In total, 229 responses were received. 26 responses with missing data and aberrant responses were excluded, yielding a total of 203 completed questionnaires for the analysis. The demographics of the studied population are shown in Table 2.

A total of 203 responses were ready for the structural equation modeling analysis. The demographical statistics of

Table 1: Construct definitions and measurement items.

Uncertainty avoidance	Rules and regulations are important because they inform students what the school or teachers expect of them. People should avoid making changes because things could get worse.	(Boss et al., 2015; Hofstede, 2011).
Subjective norm	My family members and friends believe I should take advantage of information security technology to protect my personal or working information. My professors think I should take advantage of information security technology to protect my personal or working information. My information security behavior will be affected by surrounding people.	(Ng et al., 2009; Yoon et al., 2012).
Attitude toward information security	Applying some information security measures in our daily life is a good idea. Applying some information security measures in our daily life is necessary. Applying some information security measures in our daily life is beneficial.	(Park et al., 2014)
Behavioral intention toward information security	It is my intention to apply different information security technologies into my daily life. I am certain I will use information security technology in my daily life. It is possible that I will use different information security technologies to protect my personal and working information.	(Park et al., 2014)
Behavior habit toward information security	I frequently use information security measures to protect my personal and working information. I automatically use information security measures to protect my personal and working information. I have been using information security measures for a long time.	(Moody and Siponen, 2013)
Information security behavior	In general, I use different information security measures to protect my personal and working information. I will set different passwords for different accounts or electronic devices. I will not open unknown e-mails from undetermined sources. I will read carefully about the relative protocols (such as authorization information) before installing software on mobile or computer.	(Parsons et al., 2014)

Table 2: Basic Information of the sample population.

Items	Choices	Number	Percentage (%)
Gender	male	97	45.8
	female	106	54.2
Educational attainment	College	62	30.1
	Bachelor	73	36.2
	Master	43	23.1
	Doctoral	25	10.6
Country	China	108	58.5
	Canada	80	23.5
	USA	12	8.9
	Others	3	9.1

these respondents were analyzed across their gender, educational level and country.

Table 2 shows the gender distribution of the respondents.

The proportion of men and women is about the same, 45.8 and 54.2%, respectively. It also presents an overview of the country composition of respondents, comprising 23.5% in

Table 3: Reliability and validity.

Variable	Measured item	Factor load	CR	Cronbach's Alpha	AVE	rho_A
BA	BA1	0.930	0.955	0.938	0.843	0.951
	BA2	0.939				
	BA3	0.950				
	BA4	0.849				
BE	BE1	0.894	0.929	0.899	0.767	0.909
	BE2	0.900				
	BE3	0.853				
	BE4	0.855				
BI	BI1	0.916	0.951	0.931	0.829	0.932
	BI2	0.902				
	BI3	0.909				
	BI4	0.915				
SE	SE1	0.869	0.904	0.865	0.801	0.899
	SE2	0.810				
	SE3	0.800				
	SE4	0.868				
PBC	SN1	0.877	0.906	0.861	0.808	0.867
	SN2	0.785				
	SN3	0.904				
	SN4	0.792				
UA	UA1	0.783	0.841	0.752	0.770	0.761
	UA2	0.766				
	UA3	0.799				
	UA4	0.769				

Canada, 58.5% in China, 8.9% in the United States and 9.1% in others.

As shown in Table 2, 31% of the respondents have a college degree, 23.1% of them have master's and 10.6% of the respondents have a doctoral degree. 36.2% of the respondents have a bachelor's degree.

RESULTS

Reliability, validity and discriminant validity

This employs Smart PLS to test the conceptual model. SmartPLS is one of the commonly used research tools in the field of information security to study if hypotheses have been accepted. Its strength lies in having no strict restriction on the number of target samples and the sample distribution (Chin, 1998). SmartPLS can directly generate the indicators for testing the conceptual model's reliability. Therefore, this section employs SmartPLS 3.2.7 to analyze the sample data and test the degree of reliability and validity of the questionnaire measurement scale.

In social science research, Cronbach's α(Cronbach index) and composite reliability (CR) values of the potential variables in the computational model are used commonly to gauge model reliability (Lee and Song, 2013). It is generally considered that when the values of Cronbach's α and CR are simultaneously both larger than 0.7, the measurement model has passed the reliability test (Bagozzi, 1988). Our exact results can be seen in Table 3. From values in the table, it can be seen that the Cronbach index of the measurement items within the measurement instrument is higher than 0.823 and their CR is larger than 0.870. The results indicate that the model has good reliability and the measuring standard has passed the reliability test.

Regarding convergence validity, it is generally considered that when the factor load value is over 0.7 and the average variance extracted (AVE) value of the potential variables is greater than 0.5 in the meantime, the convergence validity of measurement item indicators in the model is satisfactory

Table 4: Discriminant validity.

	BA	BE	BI	PBC	SN	UA
BA	**0.919**					
BE	0.809	**0.878**				
BI	0.820	0.853	**0.912**			
PBC	0.519	0.437	0.537	**0.837**		
SN	0.755	0.629	0.654	0.604	**0.843**	
UA	0.598	0.526	0.526	0.450	0.555	0.751

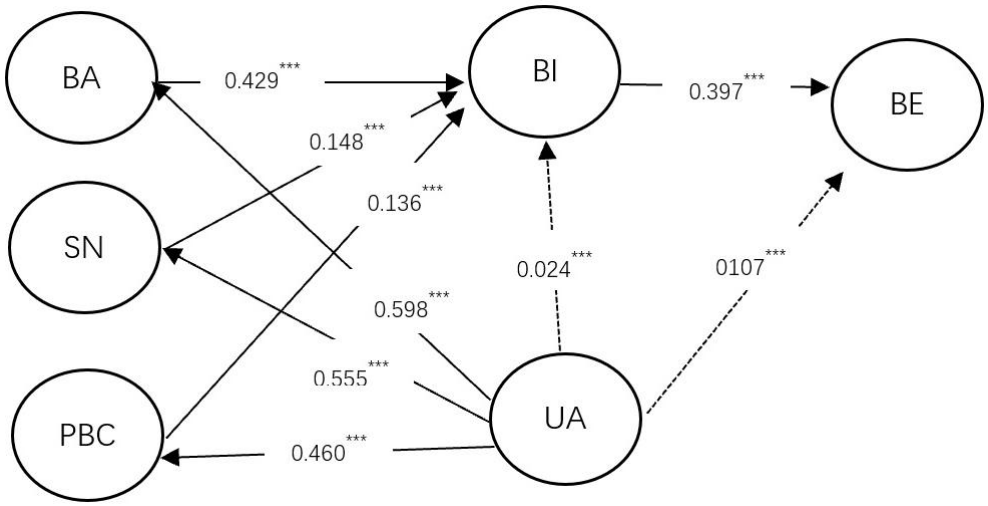

Figure 3: Path coefficients of the conceptual model.
Notes: *p<0.05, **p 0.01, ***p<0.001, ns: non-significant.

(Lee and Song, 2010). The factor load values and AVE values of the potential variables involved in the paper's measurement model are indicated in Table 3. The convergence validity has passed the test. Regarding discriminant validity, the test results are shown in Table 4. The bolded values along the diagonal line are the squares of the AVE of the variables. From the table, it can be seen that they are all higher than the correlation coefficients of the build variables with other variables correspondingly below. Therefore, there is quite a good discriminant validity between the measurement variables (Fornell and Larcker, 1981).

Structural model analysis

SmartPLS is used to test the structural equation model of this research. The test results are shown in Figure 3. To conduct T test of significance of the model, repleaded sampling by bootstrapping is commonly employed (Lee and Song, 2010). The number of repeatedly taken samples is set as 1000 (Wixom and Watson, 2011). Table 5 shows in detail the T values, path coefficients and significance test results across the variables.

The results of the data analysis indicate that among the five hypotheses, three are accepted and two rejected. Within them, the influence from UA on behavior attitude, subjective norm and perceived behavioral control are significant. Hypotheses 1, 2 and 3 have passed the test. However, hypothesis 4 and 5 failed the test, which means UA has no significant relationship with intention and behavior.

FINDINGS

According to our research on cross-cultural countries, uncertainty avoidance clearly has a significant influence on students' information security behavior. The concrete manifestations are as below:

1). UA has a positive influence on behavior attitude: The results of this survey support the hypothesis that uncertainty avoidance influences behavior attitude. This illustrates that in a national cultural environment of high uncertainty avoidance, students pay more attention to avoid unknown risks. Their attitude to taking information security behaviors tends to be more positive. This is in line

Table 5: Path coefficients, T values and hypothesis testing.

Hypothesis	Path	Path coefficient	T value	Pass / Failed
H1	Uncertainty Avoidance--behavior attitude	0.598**	7.931	Passed
H2	Uncertainty Avoidance--subjective norm	0.555***	5.833	Passed
H3	Uncertainty Avoidance--perceived behavioral control	0.450***	4.035	Passed
H4	Uncertainty Avoidance--behavioral intention	0.024	0.174	Failed
H5	Uncertainty Avoidance--behavior	0.107	1.283	Failed

with the characteristics of Hofstede delineated in the cultural dimension theory.

2). UA has a positive influence on subjective norm: The results of this survey support the hypothesis that UA influences subjective norm. This illustrates that individuals with high UA cultural background generally treat external social pressures seriously. In the national cultural environment of high uncertainty avoidance, policies, standards and social norms are their behavioral basis. Individuals with high UA tend to abide by security policies (Mladenović et al., 2017).

3). UA has a positive correlation with perceived behavioral control: The results of this survey support the hypothesis that UA influences perceived behavioral control. When users have a high degree of uncertainty avoidance, they aremore cautious in the face of risks and are more willing to participate in controllable behaviors. This conclusion differs from that of Quintal et al. (2010) on the information behavior study of Australians in travel scenarios. This is probably because when people's uncertainty avoidance increases, they tend to give up general behaviors, for instance, go traveling. However, they may be more willing to the information security protection behaviors, which can enhance their perceived behavioral control and reduce their anxiety.

4). UA has no direct impact on behavioral intention or information security behavior: Since UA has a significant impact on attitudes, subject norm and perceived behavioral control, it is clear that UA is an influential factor in information security behavior. Interestingly, however, our findings show that they do not have a direct impact on the willingness to act on information security, nor do they have a direct impact on safety behavior. The reason for this may be the direction that needs to be explored next.

DISCUSSION

Previous studies have shown that culture has a direct or potential influence on people's information behavior (Veiga, 2015; Jackson and Wangle, 2013), especially UA is considered to be an important factor (Al-Mukahal, 2015). In the present study, we further explored the impact of UA on information security behaviors through an empirical survey of 203 college students in different cultural backgrounds, and found that it does not directly, but indirectly affect information security behavioral intention, through three factors including behavior attitude, subjective norm, and perceived behavioral control.

In addition, other researchers have concluded in the context of technology acceptance that individuals with a higher UA culture are less willing to try new technology solutions to existing needs or problems (Keil et al., 2000; Veiga et al., 2001). We confirm that this relationship is still true in the context of information security behavior, that is to say, people with high UA cultural background tend to be more conservative in behavior attitude and willingness, are more willing to abide by the policies regulating information security behavior.

Limitation and future work

A couple of limitations of this study provide opportunities for future research. First, there are some regional limits of the sample. Researches on cultural factors in other countries than mainland China, Canada and USA have not been included. In future research, samples from other regions could be taken to study the applicability of the models. Also, the sample of this study is limited to college students, care must be taken when extrapolating the findings to other types of groups of users.

CONCLUSION

This is the first attempt to introduce the TPB model into the exploration of the impact of culture on information security behavior, through which the pattern of the UA's impact has been determined for the first time. It is shown that the impact of UA on information security behavioral intention is not directly generated, but indirectly generated through behavior attitude, subjective norm, and perceived behavioral control. This research helps us to better understand the cultural dimension influencing the intention of individual information security behavior. Also, it has provided theoretical support for studying the relationship between UA and individual's information security behavior even better in the future. From the practical perspective,

the conclusion of this research would be helpful for increasing our understanding of individuals' information behavior, assisting rightfully handling of variation in individuals' behaviors owing to cultural differences. It can also be of use to policy makers to formulate workable policies according to people's cultural backgrounds.

ACKNOWLEDGEMENT

This work is supported by the Natural Science Foundation of China (Grant 71473182).

REFERENCES

Ajzen I (1985). From intentions to actions: A theory of planned behavior. ActionControl, Springer,J. Kuhl et al.pp11-39.

Ajzen I (1991). The theory of planned behavior. Organ. Behav. Hum.Decis. Process. 50(2): 179–211.

Albrechtsen E (2007). A qualitative study of users' view on information security. Comput. Secur. 26(1): 276–89.

Anat H, Putri FF (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. Pervasive Mob. Comput. 32: 35–49.

Anat H, D'Arcy J (2012). Applying an Extended Model of Deterrenceacross Cultures: An Investigation of Information Systems Misuse in the U.S. and South Korea. Inf. Manag. 49(2): 99–110.

Aurigemma S, Mattson T (2018). Exploring the effect of uncertainty avoidance ontaking voluntary protective security actions. Comput. Secur. 73: 219-234.

Bagozzi RP, Yi Y (1988). On the evaluation of structural equation models: J. Acad. Market. Sci. 16(1): 74-94.

Banerjee S, Ho SS (2019). Applying the theory of planned behavior: Examining how communication, attitudes, social norms, and perceived behavioral control relate to healthy lifestyle intention in Singapore. Int. J. Healthc. Manag. pp 1–8.

Cardon P (2008). National culture and technology acceptance: The impact of uncertainty avoidance. Issues Inf. Syst. 9(2):103-110.

Cardon P, Marshall B, Norris DT, Cho J, Choi J, Cui L (2009). Online and offline social ties of social network website users: An exploratory study in elevensocieties. J. Comput. Inf. Syst. 50(1): 54–64.

Chang C-C, Chang W-L, Chin Y-C (2009). User Acceptance of Self-serviceTechnologies - An Integration of the Technology Acceptance Model and the Theory ofPlanned Behavior(2009). 11th International Conference on Enterprise Information Systems, Proceed. pp 161-164.

Cheung MFY, To WM (2017). The influence of the propensity to trust on mobileusers' attitudes toward in-app advertisements: An extension of the theory of planned behavior. Comput. Hum. Behav. 76: 102–111.

Chin WW (1998). The partial least squares approach for structural equationmodeling.In G. A. Marcoulides (Ed.), Methodology for business and management. Mod. Methods Bus. Res. pp 295-336

Choi KS, Im I, Hofstede GJ (2016). A cross-cultural comparative analysis ofsmall group collaboration using mobile twitter. Comput. Hum. Behav. 65: 308–318.

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R (2013). Future directions for behavioral information security research. Comput. Secur. 32: 90–101.

D'Arcy J, Hovav A, Galletta D (2009). User Awareness of SecurityCountermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Inf. Syst. Res. 20(1): 79–98.

Hampden-Turner C，Trompenaars F (2006) Cultural intelligence - Is such a capacity credible? Group Organ. Manag. 31(1): 56-63

Hofstede G (1993). Cultural constraints in management theories. Acad. Manag. Exec. 7(1): 81–94.

Hofstede G (2011). Dimensionalizing cultures: The Hofstede model in context. Online Readings Psychol. Cult. 2(1): 8.

Hofstede G, Garibaldi de Hilal V, Malvezzi A, Tanure SB, Vinken H (2010).Comparing Regional Cultures Within a Country: Lessons Brazil. J. Cross-Cult. Psychol. 41: 336–352.

Hofstede G, Hofstede GJ, Liyuan, Sun J (2010). Culture andOrganization:The Power of Psychological Software(Second Edition). Beijing: Renmin University of China Press.

Jackson LA, Wang J-L (2013). Cultural differences in social networking site use: Acomparative study of China and the United States[J]. Comput. Hum. Behav. 29(3): 910–921.

Junco R, Heiberger G, Loken E (2011). The effect of Twitter on college studentengagement and grades: Twitter and student engagement. J. Comput. Assist. Learn. 27(2): 119–132.

Keil M, Tan BCY, Wei K-K, Saarinen T, Tuunainen V, Wassenaar A (2000). Across cultural study on escalation of commitment behavior in software projects. MIS Q. 24(2) : 299-325.

Kim E, Lee J-A, Sung Y, Choi SM (2016). Predicting selfie-posting behavioron social networking sites: An extension of theory of planned behavior. Comput. Hum. Behav. 62: 116–123.

Lai C, Wang Q, Li X, Hu X (2016). The influence of individual espoused culturalvalues on self-directed use of technology for language learning beyond the classroom.Comput. Hum. Behav. 62: 676–688.

Lebek B, Uffen J, Neumann M, Hohler BH, Breitner M (2014). Informationsecurity awareness and behavior: A theory-based literature review. Manag. Res. Rev. 37: 1049–1092.

Lee I, Choi B, Kim J, Hong S-J (2007). Culture-Technology Fit: Effects ofCultural Characteristics on the Post-Adoption Beliefs of Mobile Internet Users. Int. J. Electron. Commer. 11(4): 11–51.

Lee SY, Song XY (2010). Structural Equation Models. Int. Encycl. Educ. 3(472): 453–458.

Parsons K, Mccormac A, Butavicius M, Pattinson M, Jerram C (2014).Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Comput. Secur. 42(4): 165–176.

Posey C, Roberts TL, Lowry PB (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. J. Manag. Inf. Syst. 32(4): 179–214.

Posey C, Roberts TL, Lowry PB, Bennett RJ, Courtney JF (2013). Insiders' protectionof organizational information assets: development of a systematics-based taxonomyand theory of diversity for protection-motivated behaviors. MIS Q. 37(4):1189–1210.

Puhakainen P, Siponen M (2010). Improving employees' compliance throughinformation systems security training: an action research study. MIS Q. 34(4):757–778.

Quintal VA, Lee JA, Soutar GN (2010). Risk, Uncertainty and The Theory ofPlanned Behavior: a Tourism Example. Tour. Manag. 31(6): 797–805.

Rhodes K (2001). Operations security awareness: the mind has no firewall, Comput. Secur. J. 18(3):27-36.

Safa NS, Sookhak M, Von Solms R, Furnell S, Ghani NA, Herawan T(2015). Information security conscious care behaviour formation in organizations. Comput. Secur. 53: 65–78.

Samhan B (2017). Security behaviors of healthcare providers using HIT outside ofwork: A technology threat avoidance perspective. Int. Conf. Inf. Commun. Syst. pp 342–347.

Shropshire J, Warkentin M, Sharma S (2015). Personality, attitudes, and intentions:Predicting initial adoption of information security behavior. Comput. Secur. 49: 177–191.

Solms RV, Niekerk JV (2013). From information security to cyber security.Comput. Secur. 38(4): 1–7.

Straub D, Loch KE, Hill C (2002). Transfer of Information Technology to theArab World: A Test of Cultural Influence Modeling. J. Glob. Inf. Manag. 9:4.

Straub DW, Welke RJ (1998). Coping with Systems Risk: Security PlanningModels for Management Decision Making. MIS Q. *22*(4): 441-469.

Straub DW, Welke RJ (1998). Coping with systems risk: security planning modelsfor management decision making. MIS Q. 22(4):441–469.

Tierney WG, Schein EH (1986). Organizational Culture and Leadership. Acad. Manag. Rev. 11(3): 677- 680.

Triandis HC (1994). Culture and social behavior. Retrieved fromhttp://www.leadershipcrossroads.com/mat/Culture%20and%20S

ocial%20Behavior.pdf.
Veiga JF, Floyd S, Dechant K (2001). Towards modelling the effects of nationalculture on IT implementation and acceptance. J. Inf. Technol,16(3):145-58.
Wang X, Zeng Y, Arntzen AA, Kim K-Y, Liu Y (2017). OrganizationalCapability: Skills Related to Organizational Knowledge. J. Integr. Des. Process Sci. 21(1): 1–3.
Wang Y, Norice G, Cranor LF (2011). Who is concerned about what? A study ofAmerican, Chinese and Indian users' privacy concerns on social network sites. InTrust Trustworthy Comput. pp 146–153.
Zhang X, Yang H (2018). Impact of Cross-culture on Behavioral Information Security. J. Integr.Des. Process Sci. pp 1-18.
Zhang X, Pablos POD, Xu Q (2014). Culture effects on the knowledge sharingin multi-national virtual classes: A mixed method. Comput. Hum. Behav. 31(1): 491–498.